


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

 **电脑报** 总策划 连续**10**年再版，累计畅销**230**万册



可启动·可杀毒

电脑报 编 **电脑硬道理** 第**10**版

网管实战


大师级
DIY

组网、用网、管网的首选指导用书

10年品牌**铸就辉煌**

- **4**大体系全面解读网管员必备知识与技巧
- **13**类近**20**种网络组建方案让你拿来就用
- **15**套典型网络应用案例让你精通局域网
- **1500**条网管技巧与应用经验打造高效网管


赠 网管精英 三个小时教程

 电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

封面设计：黄丹

电脑硬道理 第10版

装机圣手

- 硬件知识完全讲解，电脑组装、外设连接全程图解
- 电脑配件选购指南，最新电脑装机方案完全收录
- BIOS设置、硬盘分区、系统安装、网络连接面面俱到
- 电脑日常保养维护方法，电脑常见故障排除大全

电脑医院

- 故障机理全面分析，排解流程详细介绍
- 电脑安全防范指导，病毒、木马专题讲解
- 主机硬件、外设、数码产品常见故障处理
- 系统维护、软件应用、网络安全面面俱到

玩转笔记本

- 笔记本电脑基础知识，购买方法，完全掌握
- 笔记本电脑无线局域网，配置优化，自由自在
- 笔记本电脑安全加密，数码外接，快捷上手
- 笔记本电脑维修升级，保养翻新，专家指导

黑客攻防

- 新手起步 黑客必知必会的安全术语与黑客命令
- 上手实战 进程、端口、账户、密码攻防实例剖析
- 攻防对弈 木马、黑客、网站、服务器攻防高手对决
- 即查随用 1000余条黑客攻防技巧与经验倾囊相授

Windows 应用高手

- 快速体验 Windows XP系统基本操作与文件管理
- 轻松掌握 网上休闲娱乐、家庭网络平台搭建与应用
- 安全防线 注册表、组策略、杀毒工具捍卫系统安全
- 随查随用 系统备份还原、磁盘优化管理与维护技能

网管实战

- 从入门到精通，轻松掌握局域网各种知识
- 从选购到安装，详细熟悉局域网各种设备
- 从理论到实战，深入探寻局域网组建过程
- 从菜鸟到精英，我们集十年之大成伴你步步走过

分类建议：计算机/网络 维护

ISBN 978-7-8947-075-3



9 787894 760753 >

定价：32.00元（1CD+1手册）

DIY2.0，我要的生活态度

**DIY，一个由来已久的名词，早已深入人心。但DIY的真正含义，知道的人又有多少？
DIY (Do it yourself) 就是自己动手。但DIY早已不局限这个范畴，在这愈发崇尚自我的时代，DIY代表的是Design Innovation Yourself（设计、创新、个性）。架设一个量身定制的网络，探究一种新颖别致的应用方案……这，就是一种生活的态度！**

1996年，DIY的理念由《电脑报》在国内率先提出，并随即在电脑爱好者中迅速流传开来，深受电脑商家和用户的推崇，以致一批又一批电脑玩家乐此不疲。DIY甚至一度成为性价比极高的组装电脑的代名词。

透过电脑应用的发展历程不难看出，正是DIY精神的深入人心，推动了国内个人电脑应用的迅速普及。而今，随着信息技术的不断升级，信息化应用得以广泛而深入地推进，DIY也不断被赋予新的内涵，不知不觉已悄然进入到了彰显个性的DIY 2.0时代，DIY的精神进而得以发扬光大：除传统硬件的选购、组装、改造、升级DIY以外，软件/系统的潜能挖掘，网络应用的按需定制、故障怪象的诊断排除、网络黑客的有效防御、酷炫作品的完美打造……也统统被纳入了DIY的领地。新一代DIY迷们通过自己动手、自学、自助，实现一项项目标应用或任务，努力挑战想象力的极限，充分享受着DIY带来的乐趣与成就。

如果说DIY 1.0的核心在于“创造性价比”，那么DIY 2.0的核心就是“以人为本”。在DIY 2.0精神的召唤下，不仅电脑应用手段大为丰富，更多产品和服务的需求也被激发了出来。在DIY 2.0时代，可以说只有你想不到的，没有做不到的。

1999年，电脑报组织资深DIY玩家和电脑高手精心编写《电脑硬道理》丛书并适时推出，实际上将当时电脑DIY的经验和精髓结集成册，系统展现给了广大读者。

丛书自出版以来，已连续10次再版，累计发行量超过230万册。《电脑硬道理》丛书，事实上成为电脑用户及时了解最新电脑应用的风向标，也是广大电脑爱好者首选的经典电脑实战手册。

由于电脑技术更新换代快，电脑应用也不断翻新，我们广泛听取了众多电脑专家和读者的意见，并顺应目前电脑DIY的趋势和潮流，选取最受广大用户关注的电脑装机、系统操作、故障排查、笔记本应用、网管实战、黑客防范等主要应用，重新策划和编写了这套新版的《电脑硬道理 2009》丛书。《电脑硬道理 2009》丛书不仅延续了历年《电脑硬道理》的风格，更注重通俗性和易用性，《电脑硬道理 2009》每本图书都赠送了一套正版软件，每张配套光盘都加入了DOS启动功能，使其更加超值实用。《电脑硬道理 2009》旨在为广大读者提供最新鲜、最全面、最权威的电脑应用资讯和实战技巧，是广大电脑爱好者提升应用水平不容错过的一道饕餮大餐！

电脑报
2009年3月



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

阅读与进阶快速通道

图书导读

	章节名	难易度	学习成果与读者群
网络组建入门	§ 1 网络基础知识 阅读耗时：0.5小时	★	1. 了解网络的基本知识； 2. 熟悉网络搭建过程中用到的各种网络设备的选购与配置技巧； 3. 掌握操作系统的相关知识。 读者群：准网络管理员，希望了解网络的入门者。
	§ 2 网络设备认知 阅读耗时：1小时	★	
	§ 3 操作系统的选择与安装 阅读耗时：1.5小时	★★	
局域网组建实战	§ 4 组建家庭局域网 阅读耗时：1小时	★★	1. 了解家庭、网吧、企业、机关以及无线网络的组建、服务器架设过程； 2. 了解不同网络环境中的设备选择方法； 3. 学会各种网络的组建方法。 读者群：各级网络管理员，网络集成施工人员。
	§ 5 组建中小型企业网络 阅读耗时：1.5小时	★★★	
	§ 6 组建校园网 阅读耗时：2小时	★★★	
	§ 7 组建无线局域网 阅读耗时：1.5小时	★★★	
	§ 8 政府办公楼网络组建 阅读耗时：2小时	★★★★	
	§ 9 网吧局域网组建实战 阅读耗时：2小时	★★★★	
网络管理维护之路	§ 10 服务器搭建、配置与管理 阅读耗时：2.5小时	★★★★★	1. 掌握局域网中共享资源、服务器远程管理以及网络安全管理办法； 2. 熟悉网络中的各种应用与管理方法。 读者群：网络管理员，系统维护人员。
	§ 11 网络升级与优化实战 阅读耗时：3小时	★★★★★	
	§ 12 服务器远程管理与维护 阅读耗时：3小时	★★★★★	
	§ 13 局域网安全管理与维护 阅读耗时：2小时	★★★★★	
疑难排除与解决	§ 14 局域网故障排除实例 阅读耗时：3.5小时	★★★★★	1. 学会简单、扼要地分析故障原因； 2. 根据分析提供解决办法，顺心随意的用好网络。 读者群：乐于自行DIY解决故障者，网络管理员。

光盘导读

- 精品软件推荐：**ESET NOD32 安全套装（三个月免费版）、木马清除大师、Serv-U、MSN 保护盾
- 精彩视频推荐：**网络操作视频、网络故障解决视频、Vista 系统安装视频
- 丰富文字教程：**网管经验介绍、网络设备相关知识、网吧网络故障专题
- 轻松休闲时光：**小羊肖恩系列、超级马里奥系列、精美音乐作品、NOD32 精美壁纸

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



全力打造最优秀中国黑客技术资源共享平台

溜客精神：

技術共享，資源共享，資料共享

不求最好，只求較好

做中國較好的網絡安全資料站

300G成套精品教程免费下载

每月网络期刊，黑客期刊发布

请将本站推荐给更多的好友

让大家都成为溜客一员

溜客資料共享群：

访问溜客安全网最下方
查看本站最新共享QQ群

溜客网络安全技术人才培养进行中

做一个通过正道可以养活自己的黑客

从我做起，不做伪黑客

WWW.176KU.COM/VIP.HTML

目录

CONTENTS

网络基础篇

《第一章 网络基础知识》

1.1 计算机网络的功能与应用概述	2	1.4 网络协议	12
1.1.1 网络的“进化”与展望	2	1.4.1 OSI模型	12
1.1.2 网络的组成	4	1.4.2 TCP/IP协议	13
1.2 计算机网络的类型	6	1.4.3 NetBEUI协议	16
1.2.1 按距离分类	7	1.4.4 NWLink IPX/SPX兼容协议	17
1.2.2 对等式和主从式	8	1.4.5 网络协议的应用原则	17
1.3 网络拓扑结构	10	1.5 网卡的地址	17
1.3.1 总线型拓扑	10	1.5.1 TCP/IPv4地址	18
1.3.2 星型拓扑	11	1.5.2 TCP/IPv6地址	21
1.3.3 环型拓扑	11		

《第二章 网络设备认知》

2.1 网卡的选购与安装	22	2.2.2 光纤	30
2.1.1 网卡的适用种类	22	2.2.3 无线传输	31
2.1.2 网卡的选购	26	2.3 网络交换设备	33
2.1.3 网卡的安装	27	2.3.1 集线器	33
2.2 传输介质	28	2.3.2 交换机	34
2.2.1 双绞线	28	2.3.3 路由器	37

《第三章 操作系统的选择与安装》

3.1 操作系统概述	40	3.3.1 安装环境	49
3.1.1 操作系统的分类	40	3.3.2 安装实战	49
3.1.2 常见操作系统简介	41	3.4 安装 Windows Server 2008	54
3.1.3 Linux家族	43	3.4.1 准备工作	54
3.2 安装 Windows Server 2003 SP2	44	3.4.2 安装实战	54
3.2.1 硬件兼容性	44	3.5 安装 Linux	56
3.2.2 安装实战	45	3.5.1 准备工作	56
3.3 安装 Vista Ultimate	49	3.5.2 Linux安装实战	57
		3.6.3 Windows XP中卸载Linux	62

目录 CONTENTS



组网实战篇

《第四章 组建家庭局域网》

4.1 家庭网络布线	64	4.3.1 使用三机四网卡实现互联	80
4.1.1 布线基本知识	64	4.3.2 使用USB联网线组网	83
4.1.2 三室两厅布线实战	65	4.4 带路由 ADSL+ 交换机多机共享	84
4.2 双机互联方案	67	4.4.1 准备工作	84
4.2.1 通过双绞线组网	68	4.4.2 ADSL设置	84
4.2.2 通过IEEE 1394组网	74	4.5 非路由 ADSL+ 路由器共享	85
4.2.3 双机三网卡共享Internet	76	4.5.1 准备工作	85
4.3 三机互联方案	80	4.5.2 路由器设置	86

《第五章 组建中小型企业网络》

5.1 企业局域网概述	87	5.3 组建域模式局域网	94
5.1.1 功能及特点	87	5.3.1 基本知识	94
5.1.2 企业布线须知	89	5.3.2 组网实战	94
5.2 网络设计方案	90	5.3.3 软件分发	104
5.2.1 中心节点的选择	90	5.3.4 高效管理企业资源	107
5.2.2 操作系统的选择	92	5.4 企业环境中的共享应用	110
5.2.3 TCP/IP方案设计	92	5.4.1 文件共享	110
5.2.4 中型网络设计案例	92	5.4.2 共享打印机	117

《第六章 组建校园网》

6.1 校园网的功能和实施原则	119	6.3.2 软件的安装	124
6.1.1 校园网的功能	119	6.3.3 联机讨论	125
6.1.2 校园网实施原则	120	6.3.4 广播教学	126
6.2 校园网设计方案	120	6.3.5 屏幕录制与回放	126
6.2.1 设计方案	120	6.3.6 文件分发	127
6.2.2 学校网络设计案例	121	6.3.7 远程命令	128
6.3 多媒体教室	123	6.4 VPN 的实现	128
6.3.1 电子教室概述	123	6.4.1 VPN概述	128
		6.4.2 VPN实例	129

CONTENTS 目录

《《 第七章 组建无线局域网 》》

7.1 无线局域网基本知识	133	7.3.2 设置主机	143
7.1.1 什么是无线局域网	133	7.3.3 数据传输	144
7.1.2 无线漫游概述	134	7.4 组建无线路由局域网	146
7.1.3 无线局域网的构件	135	7.4.1 设置无线路由	146
7.2 组建最简单的无线对等网络	136	7.4.2 设置客户端	149
7.2.1 拓扑结构与传输介质	136	7.4.3 共享上网	150
7.2.2 双机无线组网实战	137	7.5 无线优化措施	151
7.3 使用红外线双机互联	141	7.5.1 速率的优化	151
7.3.1 安装台式机红外驱动	141	7.5.2 防干扰	152

《《 第八章 政府办公楼网络组建 》》

8.1 系统概述与需求	153	8.3 群集在服务器中的应用	160
8.1.1 政府办公网络的作用	153	8.3.1 什么是群集服务	160
8.1.2 总体设计思想	153	8.3.2 建立群集实战	161
8.2 组网方案	154	8.4 架设 SSL 网站	163
8.2.1 布线设计	154	8.4.1 安装证书服务	163
8.2.2 网络设备	156	8.4.2 配置 SSL 网站	164
8.2.3 子网划分	158	8.4.3 访问 SSL 网站	168

《《 第九章 网吧局域网组建实战 》》

9.1 网吧概述	169	9.4.4 集线器和交换机	174
9.2 组建网吧的基本结构	169	9.4.5 网吧路由器	174
9.2.1 总线型网络	169	9.5 大型网吧网络组网方案	175
9.2.2 星型网络	170	9.5.1 需求分析	175
9.2.3 树状结构的网络	170	9.5.2 网络设计原则	176
9.3 Internet 的接入方式	170	9.5.3 设备选型和预算	176
9.3.1 ADSL	170	9.6 大型网吧网络系统方案实施	177
9.3.2 光纤线路	171	9.6.1 综合布线系统布线原则	177
9.4 网吧基础硬件	172	9.6.2 操作系统安装	179
9.4.1 工作站计算机	172	9.6.3 Internet 接入设备配置	181
9.4.2 网吧服务器	173	9.6.4 计费服务管理系统	184
9.4.3 网络传输介质	173	9.6.5 CS 服务器搭建	189
		9.6.6 电影音乐服务器搭建	192

目录CONTENTS



管理维护篇

《《 第十章 服务器搭建、配置与管理 》》

10.1 用 IIS6.0 搭建 Web 服务器	196	10.2.4 设置客户端连接数	204
10.1.1 什么是Web服务器	196	10.2.5 访问FTP服务器	204
10.1.2 安装IIS6.0及Web服务组件 ..	196	10.2.6 FTP服务器的管理	206
10.1.3 配置Web组件	197	10.3 用 IIS6.0 架设邮件服务器	208
10.1.4 建立多个网站	198	10.3.1 安装组件	208
10.1.5 用IIS6.0架设ASP网站	200	10.3.2 配置POP3服务器	209
10.1.6 用IIS6.0架设ASP.net网站	200	10.3.3 配置SMTP服务器	210
10.2 用 IIS6.0 搭建 FTP 服务器	202	10.3.4 测试SMTP服务	214
10.2.1 设置默认目录	203	10.4 用 IIS6.0 搭建流媒体服务器 ..	214
10.2.2 设置FTP服务器的IP地址	203	10.4.1 架设流媒体服务器	214
10.2.3 设置访问端口	204	10.4.2 Web接口管理	217

《《 第十一章 网络升级与优化实战 》》

11.1 硬件设备升级	218	11.3.3 设定补丁类型	228
11.1.1 升级分析	218	11.3.4 下载并审批补丁	229
11.1.2 升级到100M共享	219	11.3.5 客户端设置	230
11.1.3 升级到100M交换网络	221	11.3.6 部署成功	230
11.2 操作系统升级	221	11.4 优化网络性能	230
11.2.1 升级准备工作	221	11.4.1 系统自带功能优化	230
11.2.2 开始升级系统	224	11.4.2 使用第三方软件	235
11.2.3 验证升级效果	226	11.4.3 优化网络结构	238
11.3 架设局域网升级服务器	227	11.5 审核与日志管理	238
11.3.1 什么是WSUS	228	11.5.1 审核策略的设置与应用	238
11.3.2 安装WSUS	228	11.5.2 系统日志管理与维护	240

《《 第十二章 服务器远程管理与维护 》》

12.1 远程桌面	244	12.1.3 启用远程桌面功能	245
12.1.1 什么是远程桌面	244	12.1.4 使用远程桌面功能	245
12.1.2 远程桌面所需条件	245	12.2 终端服务器	246

CONTENTS 目录

12.2.1 什么是终端服务器	246	12.4.1 远程管理打印服务器	256
12.2.2 终端服务器的建立	247	12.4.2 终端服务器的Web接口管理	260
12.2.3 组策略与终端服务器	248	12.4.3 流媒体服务器的Web管理接口	261
12.2.4 终端用户权限的设置	249	12.4.4 远程维护Web接口	261
12.2.5 终端服务器的日志审核	250	12.5 软件分发	264
12.3 配置 VPN 服务器	251	12.5.1 设置共享目录	264
12.3.1 配置VPN服务器	252	12.5.2 设置组策略	266
12.3.2 添加权限账号	253	12.5.3 在工作站中安装软件	268
12.3.3 配置VPN客户端	254	12.6 远程管理注册表与组策略	268
12.3.4 拨入VPN服务器	255	12.6.1 远程编辑注册表	268
12.4 Web 接口管理	256	12.6.2 远程管理组策略	270

《《 第十三章 局域网安全管理与维护 》》

13.1 配置防火墙保障局域网安全	272	13.3.4 影子系统保护电脑安全	300
13.1.1 防火墙简述	272	13.4 木马查杀与防范	302
13.1.2 用ISA Server部署企业级防火墙	273	13.4.1 木马防线	302
13.1.3 ISA Server应用案例	287	13.4.2 Windows木马清道夫	304
13.2 系统漏洞检查与修补	290	13.4.3 微点主动防御软件	305
13.2.1 关于MBSA	290	13.5 用户数据的安全备份	307
13.2.2 安装MBSA	291	13.5.1 系统自带备份与还原工具	307
13.2.3 检查系统漏洞并修补	291	13.5.2 同步网络文件	311
13.3 病毒、黑客防范	292	13.5.3 网络备份	312
13.3.1 网络病毒的防范	292	13.5.4 服务器数据库的备份与还原	313
13.3.2 瑞星杀毒软件	295	13.5.5 Windows服务备份	315
13.3.3 轻松备份杀毒软件病毒库	297	13.5.6 用电脑防删专家保护文件	316



故障解决篇

《《 第十四章 局域网故障排除实例 》》

14.1 网卡、网线故障排除实例	318	双网卡无法同时接入两个广域网	319
TP-LINK网卡无法正确安装	318	快速收集局域网计算机网卡MAC地址	319
RealTek 8139芯片网卡不能正常工作	318	网卡的名称中多了“2#”	319
修改网卡速率突破100米限制上网	318	USB网卡无法正确安装	320

目录CONTENTS

安装网卡后启动速度变慢.....	320	无法Ping通其他计算机	328
网卡MAC地址异常	320	IP地址与系统硬件冲突	329
多种方法解决网卡冲突故障.....	321	14.4 网络设置故障排除实例	329
网线短路导致网络通信中断.....	321	更改“远程桌面连接”的默认端口...	329
延长网线的距离.....	322	限制日志大小导致Web服务自动停止	329
双机直连无法共享上网.....	322	无法使用服务器列表.....	330
网卡灯亮却不能上网.....	322	在局域网中隐藏特定计算机.....	330
14.2 路由器、交换机故障排除实例 ...	322	查看本地计算机上的连接.....	330
用路由上网无法语音聊天.....	322	无法用计算机名访问共享资源.....	330
路由器拒绝服务.....	322	添加IPX/SPX协议提示地址相同	331
宽带路由器共享上网频繁掉线.....	323	PPPoE协议冲突	331
路由器故障导致掉线.....	323	IPX/SPX协议导致网络连接中断	331
路由器上的Link灯不亮	323	TCP/IP报告错误31	332
华为ar28-09b路由器删除路由	323	启用NetBEUI协议出现网络重名	332
文件共享响应太慢.....	323	设置IP策略拒绝用户Ping服务器	332
交换机端口不正常.....	324	使用ARP绑定默认网关	334
更换交换机后无法上网.....	324	备份网络设置.....	334
更换交换机后下载速率猛增.....	324	14.5 网络权限设置故障排除实例	334
根据交换机指示灯判断故障.....	324	禁止客户计算机修改IP地址	334
违反5-4-3规则导致网络不通	324	无访问权限导致共享打印机不能使用	335
物理链路不通导致不能连接局域网...	325	限制局域网内部指定的计算机上网...	335
14.3 网络连接故障排除实例.....	325	密码策略导致无法访问共享资源.....	335
限制客户机的上网速度.....	325	清除访问密码.....	335
划分网段限制网络通信.....	325	普通用户无法连接远程桌面.....	336
VPN连接导致工作组计算机不能访问	326	不能正常访问共享资源.....	336
网络连接不正常.....	326	14.6 其他网络配置故障排除实例.....	336
防火墙阻止网络连接.....	326	区分Net localgroup和Net group命令 ...	336
如何进行端口映射	327	列出共享文件信息.....	337
远程桌面连接超出最大连接数.....	327	远程运行安装程序失败.....	337
无法Ping通计算机名	327	利用磁盘挂接解决空间不足问题.....	337
在代理服务器上限制网络流量.....	328	网络设备停止响应导致网桥失效.....	338
限制局域网和外网间的流量.....	328	无法安装网络服务.....	338
		快速获取局域网中计算机的IP地址 ...	338

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

**你
想
换
吗
？**

www.17huan.com

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网络基础篇

第一章 网络基础知识

第二章 网络设备认知

第三章 操作系统的选择与安装



第一章 网络基础知识

20年前几乎没有人接触过网络！如今，随着计算机的普及，网络已经被用于社会的各个方面。网络极大地拓展了计算机的功能，可以帮助人们更容易、更具效率地使用计算机。以一个企业网络为例，生产、运输、计划、报价、结算、广告宣传等都可以通过使用网络环境起到事半功倍的效果。

在本书的第一章中，将为读者们解释什么是网络，以及网络的架构和技术等基本概念。这些内容不仅是每位读者都应该具备的知识，更与本书以后的内容息息相关。

1.1 计算机网络的功能与应用概述

计算机网络（NetWork）的出现，让整个世界实现了信息化共享（Sharing），人们的生活、工作方式也随之发生了巨大的变化。所谓“计算机网络”，是指：以共享资源方式相互连接起来，且各自具有独立功能的计算机系统的集合。

1.1.1 网络的“进化”与展望

从20世纪50年代初期的单机（Standalone）时代，庞大、昂贵的计算机之间的数据交流非常不便。例如，两个部门分别有一台计算机，现在因为一个业务需要两个部门共享一些数据，在以前通常需要使用N张磁盘才能完成相应的任务。

几十年过去了，磁盘的容量和读取速度已经发生翻天覆地的变化。所以，可能会有人问：“我使用大容量的优盘，不行吗？”答案是：“可以，但不够迅捷！”。不过，倘若部门间距离较远，花费在往返之间的时间就会很可观。如果多台计算机之间使用网络的话，那么无论数据要复制多少

次，只需动动鼠标就可以了。



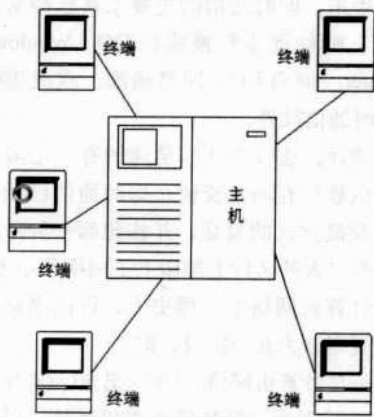
数据共享只需动动鼠标

要共享的数据容量总是在成倍的扩张，人们期待能够有一种便捷的方法实现数据的流通。日久年深，期待化成了动力，动力促进了网络的产生——动力主要来自三个方面：

- > 资源共享的需求；
- > 协作项目的需求；
- > 人力资源的节省；

第一章 网络基础知识

20 世纪 50 年代后期，随着分时系统的出现，工程师们在计算机上通过增加一个通信设备，使计算机具备通信功能。通过将远程用户的输入输出设备使用通信线路与计算机的通信设备相连，使得用户可以在远程的终端上输入自己的程序和数据，再由计算机进行处理，处理结果通过计算机的通信装置经由通信线路再返回给用户终端。



早期计算机网络的主要形式

这种系统称为具有通信功能的单机系统又称为“终端计算机”系统，是早期计算机网络的主要形式。

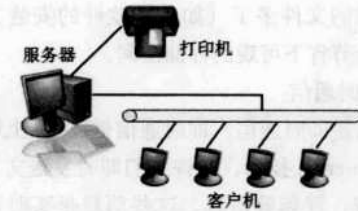
从网络雏形出现的那一天开始，网络发展就从来没有停止过脚步。特别是在我国，网络在近 20 多年中发展得很快，并逐渐成为国际网络较为发达的国家之一。通过使用网络，大大提升了工商业的运作效率。简而言之，网络的主要功能有：

* 软件数据的共享

通过使用网络，可以让数据的共享不再需要软盘、优盘、刻录盘等存储介质，进而大大减少相关硬件的购买费用。通过网络复制数据，可以让数据的流通速度更快、更稳定。此外，还可以让源数据具有惟一性。

* 硬件设备的共享

在计算机之间通过网络连接后，不仅软件数据上可以共享，在部分硬件设备上也可以共享，最常见的应用就是通过网络使用共享打印机。

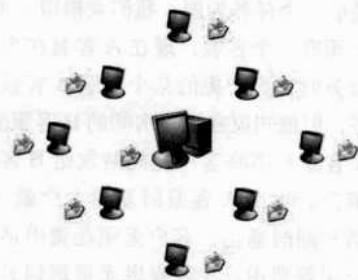


共享网络打印机

没有使用网络环境时，所有要打印的文件只能复制到连接了打印机的计算机中，再进行相应的打印任务。使用网络环境后，所有要打印的文件只需在本机中，就可以向网络里的共享打印机发送打印指令了。人们无需再为打印而奔走，数据也无需为了打印而复制、粘贴。

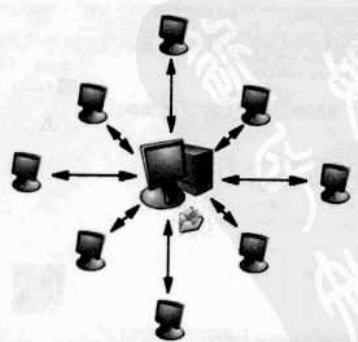
* 存储空间的节省

在单机环境中，很多计算机中的数据都是相同的。比方说，秘书制作了一份员工通讯表后，通常每位员工的计算机中都会存储一份。



大量数据重复

如果使用了网络环境，那么，秘书只需在服务器中放置一份并设置为共享，谁需要看谁就访问一下服务器就可以了。



在服务器中只保留一份数据



这样的文件多了（如各种软件的安装文件），自然就会节省下可观的存储空间。

* 即时通信

什么是即时通信？即时通信俗称“网上聊天”，它使用 Internet 技术，允许人们即时发送文本、图片、声音、视频等信息，这些消息是实时被传出去。即时通信起源于 1996 年。在这一年中，一名为 Mirabilis 的以色列人率先发布了一名为 ICQ 的免费即时通信服务。从此，各种各样的即时通信工具就层出不穷了。

即时通信至少可以帮助用户完成如下任务：

- > 即时进行文字消息交流
- > 即时进行语音聊天
- > 即时进行视频对话
- > 即时进行图片欣赏
- > 即时进行团队合作

.....

以最后一个任务为例，我们来模拟一个环境：

某公司有 3 个客服，现在 A 客服在为一个重要客户服务时，客户提的某个问题 A 客服不知该怎样回答，但他知道在另一房间的 B 客服能解答。此时，A 客服只需将客户提问转发给 B 客服，由 B 客服解答后再由 A 客服回复给客户就可以了。通过网络和即时通信，客户无须花费电话、亲自往返某公司等费用，A 客服也无须跑到另一个房间去。一切都可以由网络来完成！

现在，很多公司开会都是使用即时通信软件来完成，大家无需再正襟危坐于会议室，这样的会议效果往往更好。



即时通信用途很广

如今，即时通信（Instant Messaging）在网络中已经成为人们最主要的交流方式了，通过 QQ、Windows Live Messenger 等即时通信程序，就可以进行文字、视频、图片、声音等即时交流。由于在消息收发方面，即时通信比传统的邮件来得更快，所以人们越来越把即时通信当成不可或缺的助手。

近年来，即时通信的主要工具已经从初期的聊天室、邮件逐步转换成以 QQ、Windows Live Messenger、朗玛 UC、网易泡泡、雅虎通等为代表的即时通信软件。

据统计，迄今为止，全球约有一亿多人使用即时通信软件在网上交流。即时通信已经被认为是现代交流方式的象征，并构建起一种新的社会关系，很多人的名片上都印上了网络联系方式。

在计算机网络的发展史上，可以简单地把网络的发展划分为五个阶段，即：

第一代计算机网络：20 世纪 50~60 年代，出现了以批处理为运行特征的主机系统，以及远程终端之间的数据通信。

第二代计算机网络：20 世纪 60~70 年代，主机和主机之间、主机和远程终端之间通过前置机通信。

第三代计算机网络：20 世纪 70~80 年代，这是计算机网络发展较快的阶段，网络开始商品化和实用化，通信技术和计算机技术互相促进，结合得更加紧密。

第四代计算机网络：20 世纪 90 年代时，局域网成为计算机网络结构的基本单元，网络间互联互通的功能越来越强大，实现了资源共享、数据通信和分布处理的目标。

第五代计算机网络：21 世纪初，无线网络、千兆级网络、高速 Internet 网络已经普及，网络访问速度越来越快，网络的使用已经与人们的工作和生活紧密相连。

1.1.2 网络的组成

要组成一个网络，计算机硬件和软件系统、网络设备、网络协议这三个方面是必不可缺的。

第一章 网络基础知识

一名合格的网络管理员应该能够透彻地了解网络的组成和结构，这一点非常重要。

1. 计算机软件与硬件系统

计算机由两个部分组成，即硬件（Hardware）与软件（Software）。计算机的所有功能都是由硬件和软件共同提供的。硬件就是我们能看得见的显示器、主机（含主机内部的硬盘、CPU、主机、内板、显卡、电源等硬件）、键盘和鼠标等设备。



计算机硬件系统组成

通俗地说，软件就是可以在计算机显示器上显示出来的各种信息，如操作系统窗口、电影画面等等。计算机中的各种功能都对应对着各种的程序，如果想让计算机干什么只需运行相应的程序就可以了。

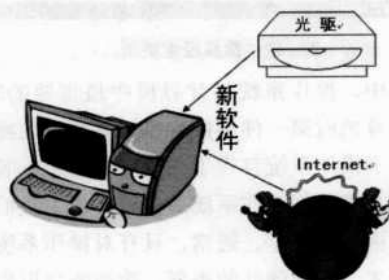
比方说，现在想用计算机看 DVD 可以吗？没问题！当我们在光驱中放入一张 DVD 电影光盘后，只需运行 Windows Media Player 或其它的播放程序即可欣赏到 DVD 光盘中的视频画面与声音了。

软件与硬件两者相辅而成，缺一不可。硬件是软件的载体，软件则是硬件的灵魂，是让硬件动起来的指挥棒！我们可以换个角度来理解硬件与软件之间的关系，比方说可以将计算机硬件看作是电视机，将软件看成是电视机中能欣赏的各个节目，通过电视塔发送过来的电视节目可以随时变换，而电视机却总是那台电视机。



软件与电视节目

计算机也是一样，计算机硬件总是由那些硬件组成，而其中的程序却可以随时更换，比方说可以更换操作系统（如将对等式网络改成主从式网络时，就需要将服务器的操作系统从 Windows XP 更换成 Windows Server 2003 或 Linux）、更换办公中使用的程序（如将国外的 Office 更换成中国的 WPS）、更换看电影的程序、更换炒股的程序等等。通常，我们可以通过光驱或 Internet 将新的程序安装到计算机中。



计算机软件来源

与买后就可以用个十年八年的空调等电器不同，计算机硬件更新速度非常快。也就是说，我们每个人的计算机硬件从买到手的那天起就已经开始了被淘汰的脚步，这是一种不可逆转的趋势，它的更新速度与软件技术的发展速度密切相关。比方说，2006 年购买的计算机在安装、运行最新的操作系统 Vista 时就会显得力不从心了。此时，对 CPU、内存或硬盘的升级几乎是势在必行的事。在一个网络环境中经常要面对各种升级的问题，升级后的网络是否能够依旧稳定、高速的运行，也是考验网络管理人员技能的一个标准。



与计算机硬件相同，计算机软件也是在不断地被更新，它的更新速度甚至还要远远超过硬件的更新速度。究其原因，主要是因为硬件有一个适用的范围，只要软件在这个范围内能够稳定运行，硬件就可以暂时不被更新。而软件不同，软件只要是不能满足人们的使用需求，就一定要进行更新。比方说，为了保证局域网中病毒防范的效果最好，杀毒程序往往就需要一天更新一次或多次，每一次的更新就会带来一个新的程序病毒库版本。



软件需要经常更新

其中，操作系统是计算机中最重要的软件。购买计算机时第一件要做的事情就是安装操作系统，由于操作系统自带了一些功能，所以装机商一般都是安装好操作系统后，就不再为我们安装其它的应用程序了。通常，只有对操作系统的大幅更新才会导致硬件的更新，普通的应用程序更新是极少需要对硬件进行更新的。



软件是计算机中一切程序和数据的统称，程序是软件具体功能的实现方式。打个比方，软件相当于“电视节目”，而程序则是电视节目中的具体频道。

因为 Windows XP、Windows Vista 等操作系统的内置了网卡、打印机、扫描仪等外围设备在内的 15000 多种硬件的驱动，所以，为计算机安装网卡等设备时，有相当一部分设备是不需要安装设备标配驱动的。

2. 网络设备

一个网络中或多或少都必须存在网络设备。网络设备有很多，视不同的网络环境、网络规模的不同而选用的网络设备也有所不同。由于在本书的第二章中，对本书中涉及的网络设备作了一个完整的介绍，故此处略。

3. 网络协议

“网络协议”就是为了让网络中的计算机能够进行相互交流的通信标准。在网络中这种标准一旦成立，就要求所有的计算机都必需遵守这个标准，才能让网络之间的交流畅通无阻！无论是组建局域网，还是访问 Internet，都需要在计算机中安装网络协议。

所以，安装了网卡等基础网络设备后，在其属性窗口总会看到一些网络协议，如 TCP/IP 通信协议等等。



网络协议必不可缺

可以说，“哪里有通信，哪里就有协议”！这就好比中国人与外国人交流时，大家如果都使用相同的语言（如英语）进行交流，那么彼此之间就可以毫无阻碍地交谈了。显然，网络协议的作用就相当于网络交流中的“世界语”——离开了网络协议，网络将无法进行相互间的交流！

1.2 计算机网络的类型

计算机网络的主要功能是向用户提供资源的共享和数据的传输，而用户本身无需考虑自己以及所用资源在网络中的位置。因此，用户只需对

Chapter

第一章 网络基础知识

网络的类型稍加理解即可。对于网络管理人员来说，通常只需掌握因特网和局域网的常见应用技术就可以了。

1.2.1 按距离分类

计算机网络分类的方法有很多，如计算机数量的规模、拓扑结构、应用协议等等。但是，这些方法都只能对网络的某方面进行区分。受到人们广泛认可的分类方法是按分布距离进行分类，即：计算机网络可以分为局域网（Local Area Network, LAN）、城域网（Metropolitan Area Network, MAN）、广域网（Wide Area Network, WAN）和因特网（Internet）。

1. 因特网

随着 Internet 网络的普及，因特网与计算机的关系越发密不可分。学计算机就要学上网，已经成为了一种趋势。通过 Internet，可以让您的网络与全世界使用 Internet 网络的计算机连接在一起，用户可以使用很多种协议对 Internet 上的资源进行访问，比方说使用 http 协议访问网站、使用 FTP 协议访问 FTP 服务器，使用 SMTP、POP 协议在邮件服务器中进行邮件收发等等。

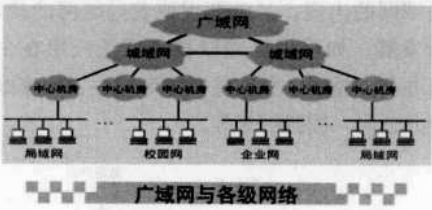


Internet 通过 TCP/IP 协议，将使用不同网络协议、不同操作系统的计算机连接到了在一起，进而构筑了一个庞大的世界性网络。

2. 广域网和城域网

对于普通用户来说，广域网这项应用显得非常陌生，只有某些大型企业才会使用这类网络。

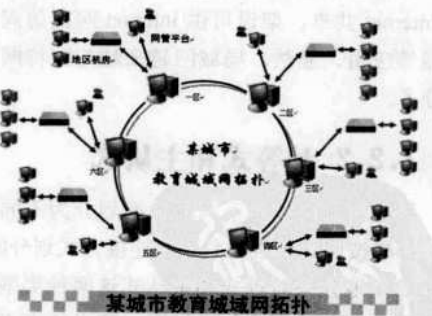
广域网也称远程网，范围在几百公里到几千公里之内。在下图中可以看出广域网、城域网、接入网以及局域网的关系。



对照 OSI 参考模型，广域网技术主要位于底层的 3 个层，分别是物理层、数据链路层和网络层。广域网作为一种跨地区的数据通讯网络，通常使用电信、移动等 ISP 提供的设备作为信息传输平台。其主要特点是：

- * 传输速度快：线路采用独享方式，保证了带宽的稳定性。
- * 保密性高：采用专线的方式，所有的数据仅在内部网内传输，最大限度的保证了传输数据的安全性。
- * 传输距离远：不受地域限制（>100KM），只要线路传输能到达的地方就能实现数据和通信的互联。

城域网使用和局域网相似的技术，可以覆盖一组邻近的大楼或一个城市（<100KM）。



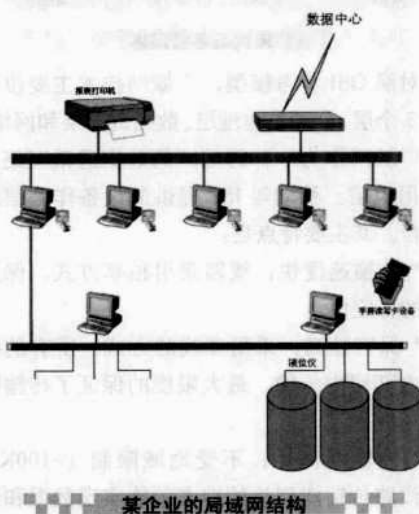
城域网既可能是私有的也可能是公用的，它支持数据和声音的传输。城域网采用 IEEE 802.6 标准，传输速率为 50kbit/s~100kbit/s。

3. 局域网

局域网指的是在一定距离（<20KM）内，将一组计算机连接起来的通讯网络。有一些局域网



称为“Intranet”，是指实现与 Internet 中一样的 Web 浏览、FTP 文件传输、论坛讨论和 E-Mail 收发等应用的局域网环境。个人计算机的普及导致了局域网的出现，并不断促使着局域网的技术在不断发展，如今的局域网技术广泛应用在企业、政府办公、校园、私人住宅等环境中，即家庭网、企业办公网、校园网等等。



局域网的特点是：覆盖范围小，速度快、误码率低，组建简单方便，成本相对低廉。

随着因特网的蓬勃发展，局域网中逐步出现了 Internet 共享，架设可供 Internet 网民访问的服务器等应用，显然，局域网越来越与因特网密不可分。

1.2.2 对等式和主从式

局域网可以按照不同的标准划分为不同的类型，如果按照计算机的关系和连接方式划分的话，可以简单地分为对等式和主从式这两种类型。无论是使用哪种类型组建局域网，都必须事先进行规划。否则，从一种类型切换到另一种类型就需要重新来过，比方说要重装不同类型的操作系统、使用不同的网络设备等。

1. 对等式

对等式 (Peer to Peer) 是最简单的局域网类型，顾名思义，在这个局域网中的计算机的关系是“平

等”的，也就是没有谁隶属于谁的概念。它们通过局域网将彼此连接到了在一起，以便实现资源的共享。



对等式局域网的特点是：

- > 数据处理能力强、工作效率高；
- > 网络的响应时间短；
- > 便于组建和进行网络扩充；
- > 数据的安全性和可靠性较差；
- > 集中管理功能较弱；

对等式局域网适合在比较宽松的环境中使用。因此，在组建局域网时，是否需要使用对等式网络就要进行斟酌。一般来说，是否使用对等式局域网主要取决于如下几点：

* 网络范围的大小

在对等式网络中不提倡计算机的数量太多，一般在 10~20 台之间为宜。因为这种网络中缺乏统一管理的机制，计算机的随意性很大。

* 操作系统

由于对等式网络的架构比较简单，所以几乎所有的操作系统都可以用来组成对等式网络，比方说 Windows 9X、Windows 2000、Windows XP、Windows 2003、Windows Vista 等等。

* 成本

使用对等式结构的局域网成本，相对于使用主从式结构的局域网要便宜些。因此，在组网经费的预算上有较严格的限制，应使用这种架构来组建网络。此外，考虑网络扩展问题，如果网络的计算机台数在较短时间内就会大量增加，就应采取具有高度可扩展性的主从式网络结构与设备。

* 管理方式

对等式与主从式的最大不同之处就在于管理方式的不同，在对等式环境中，每一台计算机的使用者都具有管理权限，包括可以自行决定是否连接到局域网。

第一章 网络基础知识

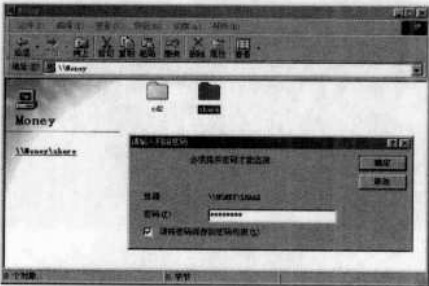


使用者有最高管理权限

在主从式网络中，客户端计算机管理员的权限级别是由服务器指定的，比方说统一更改用户登录密码的时间期限等等。

*** 安全性**

对等式网络最常见的安全性措施就是为共享资源上设定密码保护，在局域网中的任意用户，只要知道了这个密码就可以对相应的共享资源进行访问。



密码保护共享资源

因为拥有了相应的账户名和密码，就等于拥有了相应的管理权限。所以，这种安全等级被称为“Sharing Level”。在小范围的、彼此信任的局域网网络中，这种安全措施是可以有效保护资源安全的。在要求高度安全的局域网网络中，这种安全等级是不建议使用的。

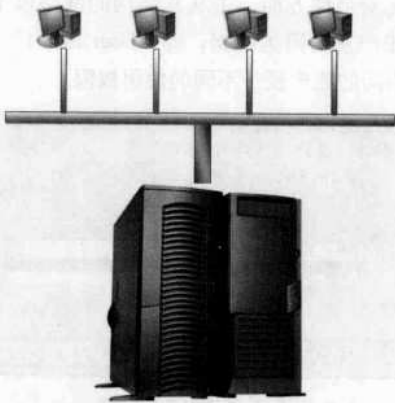
2. 主从式

一直以来，在大多数管理严格的办公和企业环境中都使用了主从式（Server/Client）网络。这是一种最为效率的网络设计，它是由少数强大的服务器（Server）来担任共享资源的提供者。



服务器

在客户端（Client）计算机中通常只安装了 Windows XP 等操作系统，并由这些计算机对服务器上的共享资源进行存取。



服务器与客户机

主从式网络的特点是：

- > 数据处理能力强、工作效率高
- > 网络的响应时间短
- > 便于组建和进行网络扩充
- > 数据的安全性和可靠性较差
- > 集中管理功能较弱

在大中型局域网网络中都需要使用主从式结构。服务器安装的操作系统一般有 Unix、Windows 2003/8、Linux 等。客户机一般安装 Windows 2000、Windows XP、Windows Vista。

在主从式结构的网络中，客户机没有任何共享资源，因为所有的共享资源都集中在少数的服务器中，这是属于集中式（Centralization）的管理

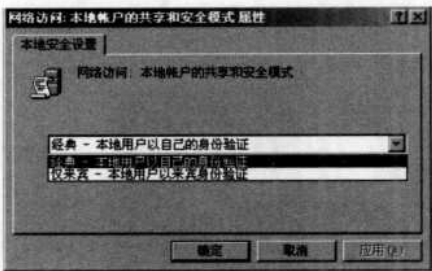


模式。因为服务器的管理和维护任务都要求具备一定的知识和精力，所以服务器一般都有专人管理以及放置在恒温的环境中，以保证它不会因为高温或随意操作而崩溃。

在服务器的所有任务（如配置、安装、升级……）中，“稳定”总是第一位的。通常，高档服务器的稳定性应高达 99.99%，平均一年内的当机时间不应超过 53 分钟。

服务器主要会存储两类内容，一是各种服务，如网站服务、FTP 服务、邮件服务、视频服务……以供内外网用户访问。二是各种共享资源，以供内网用户访问。

在安全性方面，主从式结构的网络以个人使用的账户及密码为根据，即“User Level”等级，并对不同的账户授予不同的使用权限。



以账户及密码为根据

本书以后的内容将会以一定的篇幅讲解主从式网络的管理与安全性设计，在此不再细述。

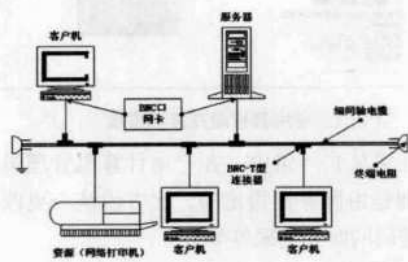
1.3 网络拓扑结构

网络拓扑 (Topology) 是网络组建中相当重要的一个名词，它是指网络上的计算机、线缆、网络设备相互连接的几何形式。如果希望一个即将组建的网络达到最佳的运行效果，就必须先设计出良好的拓扑规划。

局域网的拓扑结构常见的有总线型、星型和环型三种，只要利用这三种基本拓扑结构，就可以延伸设计出更多的拓扑结构，如树型网、簇星型网和网状网，等等。下面，将对这三种基本拓扑结构加以详细说明。

1.3.1 总线型拓扑

总线型拓扑也称直线 (Linear) 型总线，这是最简单的组网方法，也是最早出现的拓扑类型。这种拓扑结构将所有计算机均连接在一条干线 (主干或段) 电缆上。



总线型拓扑

在这种拓扑结构中，所有计算机的地位平等，无中心节点控制，计算机网络的终止取决于两端的终端电阻 (Terminator) 的所在位置。

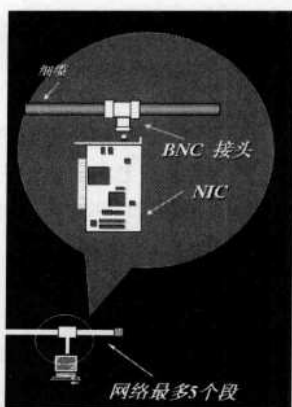


终端电阻和三通组件

当这种网络结构中的任意一台计算机传送资料时，网络上所有的计算机都会接收到此次的数据传输广播信号并进行地址检查，如果与源计算机要求的目的地计算机地址相符则接收资料。所以，只有目的地计算机才会接收到来自源计算机的资料，而其它计算机则会丢失此信号。为了阻止信号继续反弹，电缆两端必须各放置一个终端电阻，以便吸收多余的信号。

总线型结构的网络优点是：网络结构简单，电缆长度短，造价低廉且易于维护。添加计算机的操作简单、灵活，只需在任意一段电缆上添加一个三通接口，并与计算机的网卡相连就可以了。

第一章 网络基础知识

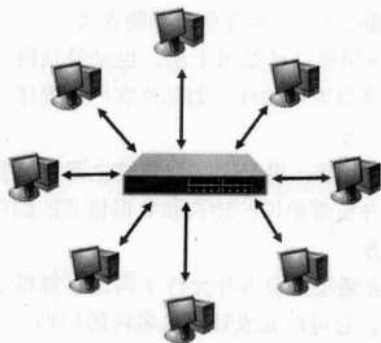


添加和减少非常简单

在一九九七年以前，我国中小规模的局域网主要都在使用这种拓扑结构，这种网络的不足之处在于分支节点故障查找比较麻烦。电缆的某一个节点发生问题时整个网络就会瘫痪，对于拥有大量计算机的网络就不适合使用这种拓扑结构。

1.3.2 星型拓扑

星型拓扑是目前使用最为普遍的网络结构，在这种网络结构中，所有的计算机都需要连接到中央部件集线器（HUB）、交换机或路由器上。



星形拓扑结构

从图上可以很明显的看出，星型网络提供了集中式的资源和管理，因此，如果中央节点出现问题，将会引起整个网络的瘫痪。如果只是其中的某一台计算机出现问题，则不会对网络上的其他计算机产生影响。

作为目前使用最多的局域网拓扑结构，星型

结构的网络特点有很多，如：

- > 结构简单，便于管理；
- > 控制容易，便于建网；
- > 成本较低，更换简单；
- > 网络延迟时间较小，传输误差较低；
- > 计算机出现故障时，不会影响整个网络；
- > 添加和减少计算机的操作非常方便；
- > 通过交换机等设备的状态灯，可以很容易判断出故障所在。

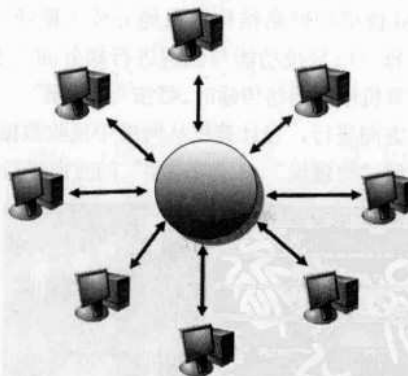
与此同时，星型结构的网络也存在着一些不足之处，如：

- > 电缆使用量，相对总线型拓扑结构来说会成倍增长；
- > 中央节点如果出现问题，则会导致整个网络瘫痪；
- > 需要额外购买中央节点的网络交换设备。

星形拓扑结构是局域网的主要发展方向，广泛应用于各类局域网，如电话网络、企业网络等等。

1.3.3 环型拓扑

在一个局域网中，所有的计算机排列成一个圆圈的方式，称为环型（Ring）拓扑。这样的网络既没有起点，也没有终点。



环型拓扑

环形拓扑结构使用一个闭合的环连接所有的计算机，这种结构不需要使用终端电阻，因为信号会沿着一个方向（顺时针或逆时针）传送，并且信号得到稳定（所有计算机的传输速度相同）。每经过一台计算机时，该计算机就“成为”中继器，



有效增强信号并将此信号传送到下一台计算机。

实际上，环形网络是由很多个点对点的电缆组合而成。当信号经过每一台计算机时，只要有一台计算机失败了，必将会影响到整个网络。当一台计算机发生问题时，信号自动向另一个方向（如逆时针）传输，尝试将数据传送任务成功完成。

环形结构的通信部件比较昂贵，所以并不常见于小型办公环境中，它主要适用于以下环境：

- > 工厂环境，因为抗干扰能力强；
- > 有大型机的场合，因为采用环形结构易于将局域网用于大型机网络中。

1.4 网络协议

本章前面的内容中已经讲解了什么是网络拓扑。在下面的内容中，将讲解一些常见的网络协议。

1.4.1 OSI模型

OSI (Open Systems Interconnection) 也称开放系统互连，它是在 1978 年由国际标准化组织 (International Organization For Standardization, ISO) 发布的一套规范，用于规定不同的设备之间相互连接的网络体系结构。通过二十多年的使用，OSI 已经成为公认的网络标准了。

OSI 模型把网络结构抽象地分成下图所示的七层，每一层是按功能与流程进行划分的。当数据从计算机中向网络传输时，将按“应用层”→“物理层”方向进行；当计算机从网络中接收数据时，则是依照“物理层”→“应用层”的方向进行。



OSI模型

为什么存在方向问题呢？比如，一个单位准备开发一个项目时，老总会安排副总主管该项目，而副总则会将任务交给某个科室的负责人办理具

体事宜，而负责人则会安排员工去收集市场信息。实际上这就是一个“数据从计算机中向网络传输”的例子。

当员工收集到市场信息，这个信息会依“员工”→“负责人”→“副总”→“老总”的顺序逐层上报，这就是“计算机从网络中收集数据”的例子。



信息收集过程

通过上述解释就可以看出，一件事需要多个“层”来协力完成，不要指望一个层就能完成所有的工作，因为这个“层”根本就忙不过来。只有分工明确，才是提高工作效率的良好方法。同样的道理，在 OSI 模型中的每一层中都有各自的任务，且每一层只和相邻的层发生通信。

下面给出了七层不同的功能含义：

- * 应用层：这是第七层，也是最顶层。它提供了网络与应用软件（如邮件客户端程序）之间的接口服务。
- * 表示层：用于定义计算机之间交换数据的格式，并负责协议的转换和数据格式的翻译、加密等任务。
- * 会话层：负责并允许不同的计算机之间建立连接。它可以完成计算机名称的识别、访问验证（如账户名和密码输入验证等操作）等任务。
- * 传输层：提供建立、维护和取消传输连接的功能，负责可靠、稳定地传输数据。TCP 协议和 SPX 协议就在此层中实现。它可以实现对会话层和网络层进行增强、加固。
- * 网络层：负责处理网络间的路由，如将数据包中的逻辑地址和名字翻译成物理地址。它可以确保数据得到及时的收发，IP 协议就在此层中

第一章 网络基础知识

实现。也就是用于确定数据可以使用哪些路径。

* 数据链路层：负责对数据包进行封装并打包成帧，执行控制数据流量、确认数据帧、检查数据帧错误（发错重传）、识别数据帧地址等任务，由此可以完成数据的无错传输。

* 物理层：这是 OSI 模型的第一层，也是最底层。它确定了电缆与网卡的连接方式，以及发送数据时使用的传输技术，在此层上传输的数据是无结构的原始数据。实际上，它用于识别网卡的硬件设置并与之进行配合。

当要传送数据给网络上其它计算机的时候，这些数据在通过当前计算机内的网卡传出去之前，会先被切割成称为“数据包 (Packet)”的数个小块后再送出去。管理员可以利用“网络监视器”来捕获当前计算机传出去的数据包，也可以捕获从其它计算机传送给当前计算机的数据包，然后通过分析这些数据包来协助诊断与解决各种类型的网络问题。

当一个数据包在 TCP/IP 堆栈 (Stack) 的各层中移动时，每一层中的通信协议都会加上自己的 header 包信息，而在加上了这些信息后，此数据包便有不同的专有名称，例如 TCP 数据包被称为 segment (段)；ICMP、UDP、IGMP、ARP 数据包被称为 message (消息)；IP 数据包被称为 datagram (数据报)；而从网络接口所传送出来的数据包被称为 frame (帧)。

1.4.2 TCP/IP 协议

网络的每一层功能都是以协议的形式描述的，协议定义了某层跟另一（远方）系统中的一个类似层（对等层）通信所使用的一套规则和约定。每一层向相邻上层提供一套确定的服务，并且由相邻下层提供的服务向远方对等层传输跟该层协议相关的信息单元。例如，传输层为它上面的会话层提供可靠的与网络无关的信息传输服务，并且使用其下面网络层所提供的服务将跟传输层协议有关的一组信息单元传送给另一系统中的对等传输层。

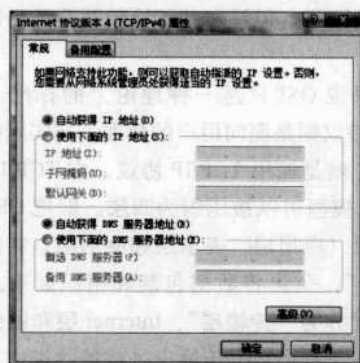
常见的网络传输协议有 NetBEUI、TCP/IP 和 IPX 等等，在下面即将讨论的 TCP/IP 通信协议是

“Transmission Control Protocol/Internet Protocol”的简写，它是目前最完整、最复杂、最庞大，但却被普遍接受的通信协议标准。TCP/IP 是一整套的数据通信协议，这个名字实际上是由 TCP（传输控制协议）和 IP（网间协议）两部分组成的。

TCP/IP 起源于 1960 年，当时美国国防部为了使他们的网络系统免受核武的攻击，因此授权 ARPA (Advanced Research Projects Agency) 研究高速的交换网络，以连接美国不同区域内的超级电脑共享彼此的资源，并在 1970 年开始使用 NCP (Network Control Protocol)。

到了 1972 年，DARPA 取代了 ARPA 的工作，并提出了 Telnet 通信协议，以及在 1973 年订立了 FTP (File Transfer Protocol) 标准。

在 1980 年，UDP (User Datagram Protocol) 标准推出，1981~1982 年间 IP 标准推出。此后，所有的计算机都必须有一个 IP 地址。



每台计算机必须有一个 IP 地址

同年，TCP/IP 协议正式由 DCA (Defense Communications Agency) 和 ARPA 提出，直到 1995 年，TCP/IP 协议才被普遍引入到个人计算机产品中，因为从那时起，Novell 和微软开始选择 IP 作为联网协议来支持其打印和文件服务的网络传输。

到了 1983 年，ARPANet 停止使用 NCP，并要求所有网络传输以及基本通信都使用标准的 TCP 和 IP 通信协议，这也是日后 Internet 广为人知的开始。

1984 年，DNS (Domain Name System) 被提出。

TCP/IP 通信协议可以将使用不同的硬件、不同的软件（如 Linux、Windows、UNIX 等）的计



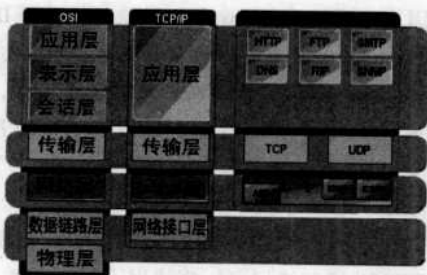
计算机实现相互的通信。如果计算机打算与网络亲密接触，就必须安装 TCP/IP 协议。TCP/IP 协议可以分为以下两种：

* 核心协议：为所有其它应用程序和其它应用层协议提供基本服务。核心协议包括 IP、APR、ICMP、IGMP、TCP 和 UDP 等。

* 应用层协议：便于数据的交换和简化 TCP/IP 网络管理，方便应用程序调用底层服务，包括超文本传输协议（HTTP）、文件传输协议（FTP）、简单邮件传输协议（SMTP）、终端仿真协议（Telnet）、域名系统（DNS）、路由选择信息协议（RIP）和简单网络管理协议（SNMP）等。

在所有的协议中，TCP 和 IP 是最重要的协议。TCP 协议提供了面向连接的字节流运输层服务。面向连接意味着两个使用 TCP 的应用在彼此交换数据之前必须先建立一个 TCP 连接。IP 协议则用于正确地将数据传送到已经使用 TCP 协议连接到的网络，但是它并不检验数据是否被正确地接收。

如果说 OSI 只是一种理论上的标准，那么 TCP/IP 协议则是面向用户的标准。在实际的网络应用中，就是使用 TCP/IP 协议。在 TCP/IP 协议中，OSI 模型可以被压缩为四层。即把 OSI 模型的上三层（应用层、表示层和会话层）共同称为“应用层”，负责将数据包装和组织起来。把它下的四层分为“传输层”、Internet 层和网络接口层，共同负责将数据传输出去或接收进来。由于 TCP/IP 协议是一整套的协议集合，所以在这四层中实际上就包含了这些不同的协议，在下图所示中，可以看到 OSI 模型、TCP/IP 协议和子协议的对应关系。



OSI模型、TCP/IP协议和子协议

1. 应用层

在应用层中提供了六项常用的协议，这些协议都可以称为“应用层协议”。



应用层协议

应用层协议支持了文件传输、电子邮件、远程登录、网络管理、Web 浏览等应用。下面，给出相应的几个协议的简介。

* HTTP

HTTP 协议又称“超文本传输协议”，它的英文全称为“Hyper Text Transfer Protocol”，这是用于在 WWW 中传输信息的协议，最常见的应用便是使用 IE 浏览器进行网页内容的浏览与下载。HTTP 地址是“统一资源地址”（URL）的一种，它的形式如：http://bbs.duze.net/。



使用http协议访问网站

HTTP 和 HTTPS 协议的不同之处，在于前者是明文传输数据的，后者是以加密方式传输协议的。

* FTP

FTP（File Transfer Protocol）协议是 TCP/IP 协议套件的一个成员，用于通过网络在两台计算机之间复制文件。

第一章 网络基础知识

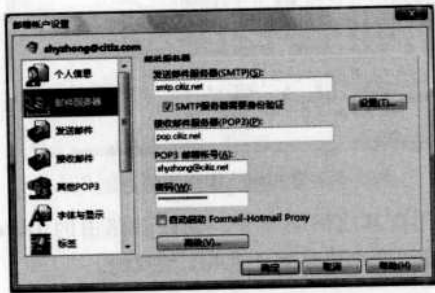


FTP数据交互

两台计算机分别扮演了两个FTP角色：一台必须是FTP客户端，另一台是FTP服务器。但这种角色并不总是一成不变。只要需要，这种角色随时都可以颠倒。

* SMTP

SMTP (Simple Mail Transfer Protocol) 即“简单邮件传输协议”。这是TCP/IP协议套件的成员之一，用于管理邮件的收发。



邮件收发

* DNS

DNS (Domain Name System) 又称“域名系统”，当我们不使用IP地址，而是使用域名对一台服务器进行访问时，就需要使用DNS服务器在网络中高速查找要访问的服务器，并由它完成域名→IP地址的转换。它最大的用处就是方便我们记忆一些网站或服务器的名称。

* RIP

RIP (Routing information Protocol) 即“路由器信息协议”，它的作用很简单，就是控制了数据通过哪些网络路径。

* SNMP

SNMP 即“简单网络管理协议”，这是一种用于监视网络的协议。

2. 传输层

在传输层中有两个非常重要的协议，它们分别是TCP和UDP。它们属于TCP/IP协议的“核心协议”。

TCP (Transmission Control Protocol, 传输控制协议) 协议和UDP (User Data Protocol, 用户数据报协议) 协议都可以用于数据传输。两者的主要区别在于两者的传递方式可靠程度不同。TCP协议中包含了专门的数据传递验证机制，当数据接收方收到发送方传来的信息时，会自动向发送方发出确认消息，发送方只有在接收到该确认消息之后才会继续传送其它信息，否则将一直等待并直至收到确认信息为止。

下图所示图形中包含了三次握手的过程示意，我们就可以看出一个TCP连接是经过三次握手协商后，连接信息才建立起来。整个会话由一个SYN包开始，然后是一个SYN/ACK包，最后是一个ACK包，此时，会话才建立成功并发送数据。



三次握手

以A机向B机传送文件为例，B机要不断地向A机发送验证数据。这个交互数据的过程在实际执行的过程中会占用系统资源，进而在一定程度上会对数据的收发速度产生影响，但却可以保证已经接收的数据与源数据并无差异。故而，对可靠性要求高的数据通信系统往往使用TCP协议传输数据。

与TCP协议不同，UDP协议并不提供数据传送的验证机制，在整个文件传输过程中如果出现数据报的丢失，协议本身并不能做出任何的检



测或提示。因此，通常人们把 UDP 协议称为不可靠的传输协议。UDP 协议适用于无须应答、要求时效的软件使用，如网络电视的应用就适合使用 UDP 协议。

那么，UDP 协议就没有可靠性而言了吗？事实上，UDP 协议也是有一定的可靠性的，只不过它的可靠性是由应用层来负责罢了。

3. 网络层

在网络层中同样有四个重要的协议，它们分别是 ARP、IP、IGMP 和 ICMP。下面，同样给出这几个协议的简介。

* ARP

ARP (Address Resolution Protocol) 即“地址解析协议”。实际上，ARP 就是获得同一个物理网络中的硬件主机地址的协议。我们知道，网卡既具有 IP 地址也有 MAC 地址，在不同的协议中不能同时使用这两个地址，而只能使用其中之一。这两个地址的提供就是由 ARP 寻找出来并提供的。此协议的名称 ARP 实际上也是一个命令行中可以使用的命令。在本书以后的内容中给出了关于 ARP 命令的内容详解。

* IP

IP (Internet Protocol) 是 TCP/IP 协议套件中的可用路由协议，它负责 IP 地址寻址、路由选择和 IP 数据包的分割和组装。这是非常重要的协议，这一点只需从 TCP/IP 这个名称就包含了 IP 协议这一点就可以看得出来。

* IGMP

IGMP (Internet Group Multicast Protocol) 即“Internet 组管理协议”，该协议运行于主机和主机直接相连的组播路由器之间，是 IP 主机用于报告多址广播组成员身份的协议。我们可以一方面通过 IGMP 协议通知本地路由器希望加入并接收某个特定组的信息；另一方面，路由器通过 IGMP 协议周期性地查询局域网内某个已知组的成员是否处于活动状态。

IGMP 协议的主要作用是解决网络上广播时占用带宽的问题。在网络中，当给所有客户端发出广播信息时，支持 IGMP 的交换机将会广播信

息不经过滤地发给所有客户端。但是这些信息只需要通过组播的方式传输给某一个部分的客户端。

* ICMP

ICMP (Internet Control Message Protocol) 即“Internet 控制消息协议”。它是 TCP/IP 协议套件中的子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

我们在网络中经常会使用到 ICMP 协议，如经常使用的用于检查网络通不通的 Ping 命令，这个“Ping”的过程实际上就是 ICMP 协议工作的过程。



使用Ping探测本机

还有其它网络命令，如跟踪路由的 Tracert、Pathping 命令也是基于 ICMP 协议的。

1.4.3 NetBEUI协议

NetBEUI 是“NetBIOS Extended User Interface”的简写，其意思是“NetBIOS 增强型用户界面”，又称 NetBIOS 扩展用户接口。NetBIOS 协议最初是由 IBM 公司在 1985 年推出，用于实现多台计算机之间的连接通信，但在使用中发现其存在一些缺陷和不足，后来经过微软公司对其进行改进和扩充，最终形成了 NetBEUI 通信协议。

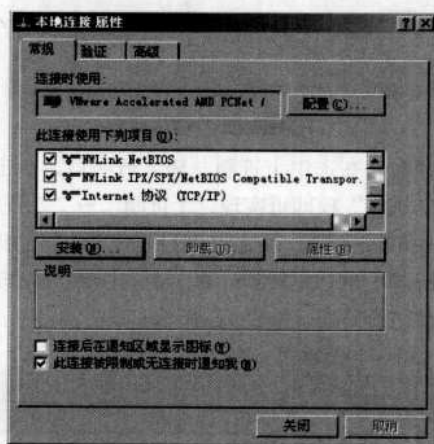
作为一个体积小、效率高、速度快、占用内存少的网络协议，NetBEUI 特别适用于局域网等小型网络。在 Windows XP 及以前的计算机中，经常需要安装 NetBEUI 协议以解决局域网中的一些应用问题。

第一章 网络基础知识

但是，因为此协议出现得比较早，所以，它也有一定的局限性。比方说，它不具备跨网段工作的能力，也就是说它不具备路由功能。因此，如果在一台服务器或计算机上安装了多块网卡作网桥时，就不能使用此协议作为通信协议，这一点必须记清楚。

1.4.4 NWLink IPX/SPX兼容协议

在 Windows NT/2000/XP/2003 中，Microsoft 提供了两个 IPX/SPX 的兼容协议，即“NWLink IPX/SPX 兼容协议”和“NWLink BIOS”，两者统称为“NWLink 通信协议”。



NWLink IPX/SPX兼容协议

Microsoft NWLink 通信协议是与 Novell NetWare IPX/SPX 兼容的网络协议。它的优点在于提供了与 Novell NetWare 的兼容性，其缺点是在小型的网络上，运行速度没有 NetBEUI 那样快，但它在设计一开始就考虑了多网段的问题，因此具有强大的路由功能，从而可用于跨网段的局域网中。

1.4.5 网络协议的应用原则

在组建网络时，具体选择哪一种网络协议主要取决于网络应用目的、网络间的兼容性和网络管理等方面。要注意的是，因为每个协议都要占用计算机的内存，因此选择的网络协议越多，占用的计算机内存也就越多。这样既影响了计算机

的运行速度，又不利于网络的管理。因此，只安装所需的网络协议是选择网络协议的基本准则。通常来说，网络协议的应用，则按如下思路进行选择：

- > 组建简单型局域网的话，NetBEUI 通讯协议是必不可少的；

- > 组建需要跨网段操作（如使用路由器或者多网卡等）的网络，NWLink IPX/SPX 兼容协议则当仁不让；

- > 组建较大的网络，并且需要接入 Internet 网络，TCP/IP 协议则是重中之重。

1.5 网卡的地址

网卡是让计算机与网络联通的网络设备，它对应了 OSI 模型中的“物理层”。在网卡中有两种地址，一是 IP 地址，二是 MAC 地址。计算机在网络中的身份以及通过网络被管理时，都离不开这两个地址的协助。

在 TCP/IP 的网络上，每一台连接到网络的计算机都被称为“主机”（Host），而主机与主机之间的通信则是由三个主要部件完成的，即：IP 地址（IP Address）、子网掩码（Subnet mask）和 IP 路由器（IP Router）。

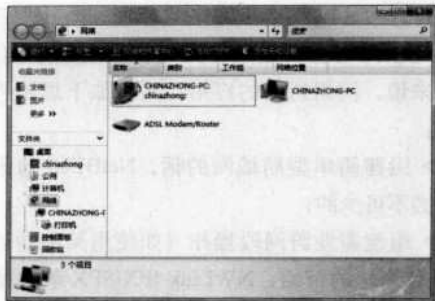
在以 TCP/IP 为通信协议的网络上，每一台主机都有一个唯一的 IP 地址，它就象计算机的门牌号码，不能与其它计算机的相同。此外，每个 IP 地址还隐含着如何在网络间传送信息的路由信息（Routing Information）。

以 Vista 为例，该操作系统支持 TCP/IPv4 和 TCP/IPv6 两种版本的 IP 地址。对于它们的管理可以通过很多种方式来完成。通常，都是在使用如下方法的任一种打开“网络连接”窗口后，通过“本地连接”（即第一块网卡）提供的设置功能来完成相关的管理任务。

- * 在“开始”菜单的“搜索”栏中，输入命令“Ncpa.cpl”并按下 Enter 键。

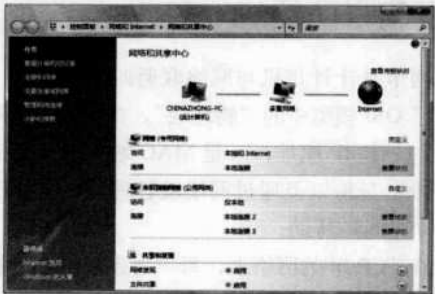
- * 在“开始”菜单中单击“网络”菜单，在打开的“网络”窗口中单击“网络和共享中心”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



网络和共享中心

在接着打开的“网络和共享中心”窗口中，单击左侧任务列表中的“管理网络连接”项。



单击“管理网络连接”

使用上述任一种方法，均可以打开“网络连接”窗口。

1.5.1 TCP/IPv4地址

TCP/IPv4 中的 IP 地址是由 32 位二进制数字组成的，并且每 8 位被分成一组，一共 4 组。组与组之间由半角句号（俗称“点”）分开，这种书写方法叫做点分表示法。为了便于人们记忆，每组数字一般都是以十进制数字标识，如 202.102.48.141（从左到右的读法）。这个 32 位的 IP 地址内包含了 Network ID（网络部分）和 Host ID（主机部分）两部分信息。

> Network ID：网络识别码，每一个网络都有

一个唯一的网络识别码；
> Host ID：主机识别码，同一个网络中的每一台主机都必须有一个唯一的主机识别码。

要进行二进制与十进制之间的数字换算，需要在“开始”菜单中依次单击“所有程序”→“附件”→“计算器”，在打开的计算器窗口中依次单击“查看”→“科学型”。在切换到的下图所示的窗口中，即可进行相应的换算。



“科学型”计算器

此时，在选中十进制并输入数字后，单击选中“二进制”项即可实现“十进制”→“二进制”的数据转换计算。反之，则可以实现“二进制”→“十进制”的数据转换计算。在进行转换操作时，要分组进行转换，如表 1-1 所示。

表 1-1 换算数据

	11001010	11001110	110000	10001101
	202	102	48	141

IP 地址可以分为 A、B、C、D、E 五类。通常，使用的 IP 都属于 A、B、C 三类，而 D、E 网则用于特殊用途，并且不使用和 A、B、C 类网具有相同的规律。

在 A、B、C 三类 IP 地址中，使用了不同长度的网络部分和主机部分来表示地址，在如表 1-2 所示中可以看到三类 IP 地址中四组数据的使用区别。由于每个 IP 地址的网络部分数字决定了它默认的子网掩码，所以清楚地知晓网络部分和主机部分的数字范围是十分有必要的。

表1-2 IP地址的结构

IP类型	IP地址	网络部分	主机部分	网络范围	主机范围	总范围
A	w.x.y.z	w	x.y.z	1~126	126	16777214
B	w.x.y.z	w.x	y.z	128~191	16384	65534
C	w.x.y.z	w.x.y	z	192~223	2097152	254
D				224~239		
E				240~254		

第一章 网络基础知识

对于专业的网络管理人员来说，需要知晓以下知识：

A 类地址：适合于超大型的网络。在将 IP 地址分为 w.x.y.z 四个组（即四个字节）时，其中的 w 是其网络部分，w 值的可用范围是 1-126，所以能够提供 126 个 A 类的 Network ID。而主机部分是 x.y.z 三个字节（1Byte=8bit），因此 24 位可以支持 $(2^{24}) - 2 = 16777216 - 2 = 16\ 777\ 214$ 台主机。

B 类地址：适合于大、中型网络，其网络部分占用 w.x 两个字节，由于 w 的可用范围是 128-191，因此可以提供 $(191 - 128 + 1) \times 256 = 16\ 384$ 个 B 类的 Network ID。而主机部分共占用 y.z 两个字节，因此每个网络可以支持 $(2^{16}) - 2 = 65536 - 2 = 65\ 534$ 台主机。

C 类地址：适合办公及家庭小型网络，其网络部分占用 w.x.y 三个字节，由于 w 的可用范围是 192-223，所以它可以提供 $(223 - 192 + 1) \times 256 \times 256 = 2\ 097\ 152$ 个 C 类的 Network ID。而主机部分只占用 z 一个字节，所以每一个网络只能使用 $(2^8) - 2 = 254$ 台主机。

D 类地址：这个 Network ID 具有特殊的用途，它是一个“多点传播”（Multicast）所使用的群组（Group ID），这个群组内包含多台主机，其 W 值的范围是 224-239。

E 类地址：这是一个专供试验室用的 Network ID，其 W 值的范围是 240-254。

现在来解释一下上述计算中的一些可能会让读者们困惑的地方：

困惑 1：127 为什么不能是 Network ID？这是因为 127 是一个保留的地址，它表示本机地址，主要用于测试网卡与驱动程序是否正常运行。

困惑 2：为什么要减 2？这是因为每一个网络的第 1 个是代表网络本身，最后一个 IP 地址代表广播地址，这两个地址不能被主机使用，所以要减去 2 才能得到实际上可以使用的主机台数。以 192.168.1.0 这个 C 类网络为例，192.168.1.0 就是网络本身，而主机部分则为 192.168.1.1~192.168.1.254，192.168.1.255 是保留给广播用途的。

最后，再来说说一些特殊的 IP 地址。这些 IP 的出现都具有不同的含义，如，有些 IP 的出现就

表示网络环境已经出现了问题。

(1) 0.0.0.0

严格说来，0.0.0.0 已经不是一个真正意义上的 IP 地址了。它表示的是这样一个集合：所有不清楚的主机和目的网络。这里的“不清楚”是指在本机的路由表里没有特定条目指明如何到达的 IP 地址。

(2) 224.0.0.1

组播地址，注意它和广播的区别。从 224.0.0.0 到 239.255.255.255 都是这样的地址。224.0.0.1 特指所有主机，224.0.0.2 特指所有路由器。这样的地址多用于一些特定的程序以及多媒体程序。如果计算机开启了 IRDP（Internet 路由发现协议，使用组播功能）功能，那么计算机的路由表中应该有这样一条路由。

(3) 169.254.x.x

如果计算机使用了 DHCP 功能自动获得一个 IP 地址，那么 DHCP 服务器发生故障，或响应时间太长超出了系统规定的时间时，系统会为计算机分配这样一个地址。

(4) 私有 IP 地址 (Private IP)

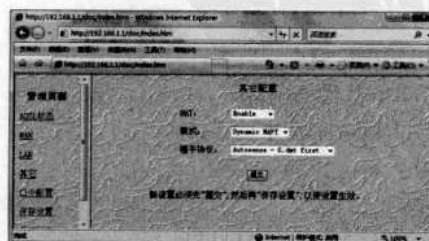
在 ABC 三类网中，如下三段网络地址为私有 IP 地址段，任何人都可以自行在自己的局域网中使用这些 IP 地址。

* 10.0.0.1~10.255.255.254

* 172.16.0.1 ~ 172.31.255.254

* 192.168.0.1~192.168.255.254

这些地址被大量用于内部网络中，一些交换机、路由器也往往使用 192.168.1.1 作为缺省地址。私有网络由于不与外部互连，因而只能够在内部网络中使用。如果要使用私有地址接入 Internet，需要使用 NAT（Network Address Translation，网络地址转换技术）将私有地址翻译成公用的合法地址。



NAT功能需要激活



除了 IP 地址外，网卡还有一个 MAC 地址，这是一个 48 位的二进制地址，它常用 12 位的十六进制表示。这是网卡的物理地址，也是绝不重复的地址。在交换机等网络设备或一些专业的网络管理软件中，都是使用 MAC 地址对计算机进行集中管理的。

在“命令提示符”窗口中，可以使用“IPconfig”命令可以查看当前计算机的网卡 IP 地址。



查看本机的IP地址

可以使用“IPconfig /all”命令可以查看到网卡的 IP 地址与 MAC 地址。



IP地址与MAC地址

通常，命令执行后会得到如下信息，其中以粗体显示的“物理地址”就是 MAC 地址、IPv4 和 IPv6 地址：

```
C:\Users\chinazhong>ipconfig /all

Windows IP 配置

主机名 . . . . . : chinazhong-PC
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
以太网适配器 本地连接 :
    连接特定的 DNS 后缀 . . . . . :
    描述 . . . . . : Realtek RTL8168/8111
    物理地址. . . . . : 00-12-35-00-00-00  MAC地址
    IP 地址. . . . . : 192.168.118.3  IP地址
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :
```

```
Family PCI-E Gigabit
Ethernet NIC (NDIS 6.0)
物理地址 . . . . . : 00-19-DB-5F-96-BA
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
本地链接 IPv6 地址 . . . . . : fe80::e9cf:638b:
d437:4cd6%8( 首选 )
IPv4 地址 . . . . . : 192.168.1.170( 首选 )
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2009 年 2 月 4 日
10:03:56
租约过期的时间 . . . . . : 2009 年 2 月 5 日
14:12:36
默认网关 . . . . . : 192.168.1.1
DHCP 服务器 . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 201333211
DNS 服务器 . . . . . : 192.168.1.1
TCP/IP 上的 NetBIOS . . . . . : 已启用
```

MAC 地址是可以进行修改的，以在 Vista 中更改 MAC 地址为例。需要使用如下方法：

首先，在“开始”菜单的“搜索”栏中，输入命令“Ncpa.cpl”并按下 Enter 键打开“网络连接”窗口。


在“网络连接”窗口中右键单击要更改 MAC 地址的“本地连接”，并进入其属性窗口。在这里可以看到有“Internet 协议版本 6 (TCP/IPv6)”和“Internet 协议版本 4 (TCP/IPv4)”两种 IP 地址。



同时支持两种IP地址版本

第一章 网络基础知识

接着，单击“连接时使用”项右侧的“配置”按钮，在弹出的下图所示属性窗口中单击选中“高级”选项卡界面中的“网络地址”项。单击选中右侧的“值”，并输入新的MAC地址（如000AE46411A1）。

**注意**

输入的MAC地址不能有“-”符号，如不能输入“00-0A-E4-64-11-A1”这种格式，正确的输入格式为“000AE46411A1”。

最后，单击“确定”按钮并重启计算机使修改生效即可。

1.5.2 TCP/IPV6地址

目前，IP地址几乎使用IPv4的版本。IPv4是一个令人难以置信的“奇迹”式的协议，它成功地把各种网络上众多的主机连接到一起，并在Internet上连接了全球数以千万计的计算机。

IPv4最多可以标识约43亿台主机，所有的IP地址都是由专门的组织（ICANN）负责的。尽管IPv4成功构筑了网络的“一级公路”，但是辉煌的日子总不会很长，IPv4的IP地址终于出现不能满足使用需求的匮乏现状，并且被要求尽快进行升级，新版的IPv6可以使用128位来表示IP地址，其容纳的IP地址数量之多，让人们戏称“连地球上的每粒沙子都可以有个IP地址”。

早在Windows XP中配置网络协议时，网络管理者们就已经把IPv6的概念对人们进行灌输了。



Windows XP中已经支持IP v6

什么是TCP/IPV6？Internet协议版本6(IPv6)是一个协议集，用于计算机通过Internet以及家庭和商业网络交换信息。IPv6的概念于1996年被提出，1998年被批准。IPv6的变化体现在IP地址扩展、身份验证和保密等方面。

通常，对于普通的家庭和小型办公用户来说，是不需要使用TCP/IPV6的。因为TCP/IPV4的地址已经完全够用。以Vista为例，系统默认已经支持IPv6，这表示我们可以将IPv4地址与IPv6地址在Vista中同时使用——虽然对于绝大多数的用户来说并无必要。

在“命令提示符”窗口中使用Ipconfig /all命令后，在得到的信息中可以看到IPv6的地址形式——IPv6地址由以冒号分隔的八组十六进制字符（数字0到9，字母A到H）构成，例如3ffe:ffff:0000:2f3b:02aa:00ff:fe28:9c5a。



IPv6的IP地址

通常，用户可以自由决定取消每个部分中的前导零，例如3ffe:ffff:0:2f3b:2aa:ff:fe28:9c5a。

那么，为什么某些IPv6地址中含有双冒号呢？其实，双冒号表明已取消了仅包含零的那部分地址，从而使地址更短。例如，fe80:0:0:0:2aa:ff:fe9a:4ca2这个IPv6地址，就可以根据需要将其写为“fe80::2aa:ff:fe9a:4ca2”。

除非有必要，否则我们在目前的网络环境中只需了解TCP/IPV6是什么就可以了，一般不必去对其进行设置。

第二章 网络设备认知

在组建局域网时，各种各样的网络设备是必不可少的。作为一名网络技术人员，不仅要能熟悉这些设备，还应能熟练地使用这些设备组建出各种规模的局域网，以及通过这些设备管理、维护局域网。

在本章中，将讲解本书涉及的一些网络设备的工作原理、选购方法，以及一些使用上的要点。

2.1 网卡的选购与安装

网卡也称“网络适配器”（NIC，Network Interface Cards）或“网络接口卡”，这是用于将计算机与网络进行物理连接的基本硬件设备，其性能的优劣将直接影响到网络效率的高低。网卡的基本功能包括：数据转换、包的装配和拆卸、网络存取控制、数据缓存和网络信号等等。

2.1.1 网卡的适用种类

网卡按照适用类型的不同，大致可以分为台式机网卡、笔记本网卡、服务器网卡和无线网卡4种。下面，分别予以介绍：

1. 台式机网卡

以太网（Ethernet）指的是由 Xerox（施乐）公司创建并由 Xerox、Intel 和 DEC 公司联合开发的局域网规范。也就是说，以太网不是一种具体的网络，而是一种技术规范。该规范定义了局域网（LAN）中采用的线缆类型和信号处理方法。90 年代，交换型以太网得到了快速发展，并先后推出了 100 兆（单位为 Mbps）的快速以太网、

1000 兆的千兆以太网和万兆以太网等更高速的以太网技术。以太网的帧格式特别适合于传输 IP 数据包。

目前，大约有 80% 的网络是采用以太网技术。所以，现在最常见到的就是以太网网卡。按网卡所支持带宽的不同可分为 10Mbps 网卡（已经停产）、100Mbps 网卡、10/100Mbps 自适应网卡、1000Mbps 网卡等几种。10Mbps 网卡已逐渐退出历史舞台，而 100Mbps、10/100/1000Mbps 自适应网卡目前是普通计算机上常用的以太网网卡。

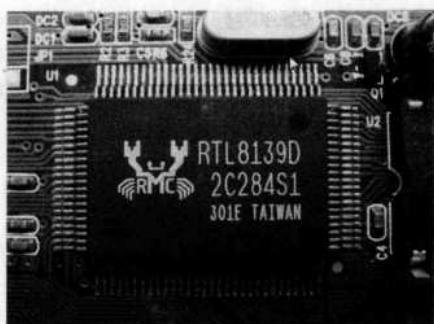
台式机使用的网卡有多种，一种是使用 PCI（Peripheral Component Interconnect）等插槽式的，另一种是主板内置式的，还有一种是 USB 等外置式的。

（1）PCI 系列

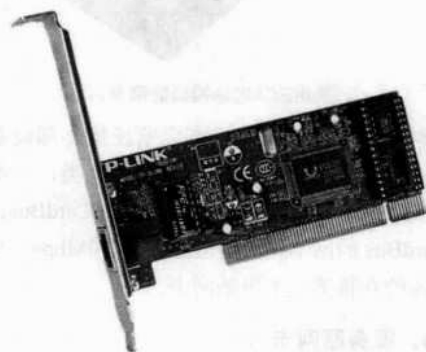
多年来，使用 PCI 插槽（即俗称的“扩展槽”）式的网卡最为常见，其价格从 20 多元到数百元不等，其主要区别是传输速度、使用的芯片、附加功能有所不同。目前，50 元以下产品中使用最多的就是 TP-LINK TF-3239D 系列，其使用的是 Realtek RTL8139D/8169 网络芯片，具

第二章 网络设备认知

备 10/100Mbps 自适应传输速度、使用 PCI 总线、RJ-45 接口、支持网络唤醒和网络启动功能。



网卡使用的芯片

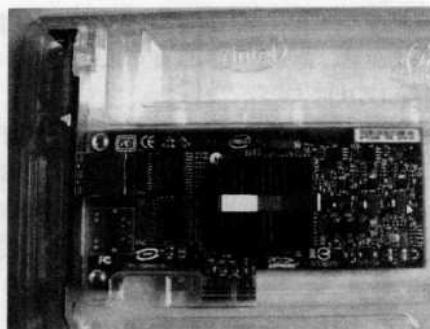


TP-LINK TF-3239D系列网卡

PCI 总线可以提供 32 位、33MHz 的带宽，数据传输量为 133Mbps/S，随着网络技术的发展，这种老式总线已经不够满足速度传输的需求了。从 1992 年的 PCI 1.0 到最新的 PCI 2.0、PCI2.1、PCI2.2、PCI2.3、PCI3.0，PCI 总线技术已经度过了 12 年，也许在不久的将来它就会因为 PCI-E 总线的盛行退出历史的舞台。

(2) PCI-E

除了 PCI 插槽外，Intel EXPI9300PT 等网卡还使用了 PCI-Express 1X（简称 PCI-E）接口，这种类型的网卡数据传输标准速度可以达到 250MB/S（每秒）、双向速度 500MB/S。使用 PCI-Express 接口的网卡多为千兆网卡。

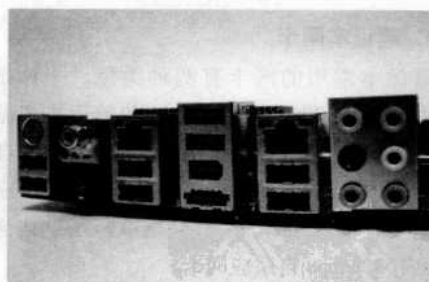


使用PCI-Express接口的网卡

PCI-Express 接口除了 1X 外，还有标准速度为 500MB/S 的 2X，标准速度为 1GB/S 的 4X，标准速度为 2GB/S 的 8X，标准速度为 4GB/S 的 16X。正因为 PCI-Express 有着如此高的传输速度，所以，它能够为千兆以太网网卡、基于 Ultra SCSI320 的磁盘阵列控制器等具有高数据吞吐量的设备提供足够高的带宽支持。

(3) 内置网卡

现在，很多主板都内置了网络芯片，并提供相应的 RJ-45 插槽，我们只需在网线上压好水晶头，将水晶头插入 RJ-45 插槽就可以了。内置网卡的传输速度从 10/100Mbps~1000Mbps 的都有，但目前主流芯片都是 Realtek 8111B 这样的千兆网络控制芯片。



内置网卡

和以前内置网卡性能远不如独立网卡不同，如今很多用料充足的主板，内置的网卡性能都不亚于同速率的某些独立网卡。如华硕 P5Q SE(ASUS P5Q SE) 这款中低档主板就内置了千兆网卡，在使用过程中网速一直很稳定。内置网卡



和独立网卡在使用上并无不同之处，它们都需要安装网卡驱动，都是连接网线就可以使用了。

(4) USB 网卡

通过 USB (Universal Serial Bus, 通用串行总线) 端口，可以协助计算机非常方便地与外部硬件（如优盘、存储卡、MP3、数码相机等）进行高速连接。USB 端口最大的特点就是支持即插即用。

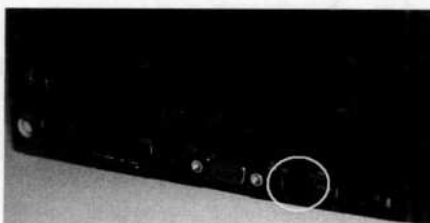
如今，USB 网卡有两种类型，一种是 USB 无线网卡（见本章后面内容）；另一种是 USB 转 RJ45 网卡线，也就是将 USB 口一端插入计算机的 USB 插槽，另一端插入网线的水晶头，通过其中的网络芯片可以实现网卡的功能。



USB 转 RJ45 网卡线

2. 笔记本网卡

笔记本常用的网卡有两种类型，一种是内置的网卡，从 2001 年以后生产的笔记本电脑中都内置了网卡。内置网卡从 10/100Mbps 自适应、100Mbps 网卡、10/100/1000Mbps 自适应等类型都有。如 ThinkPad X200 这款机型就内置了 10/100/1000Mbps 自适应网卡。



笔记本内置网卡

对于一些老式笔记本电脑或网卡数量不够用、内置网卡已经损坏、希望使用外置无线技术的笔记本电脑来说，还有两种网卡的使用选择，一是前面介绍过的 USB 式网卡；二是使用 PCMCIA 接口的网卡，下图是价值 120 元的 TP-LINK TG-5269 这款 10/100/1000Mbps 自适应网卡。



使用 PCMCIA 接口的网卡

PCMCIA 接口是笔记本电脑连接外部设备的一种主要方式，PCMCIA 接口分为两类，一类是 16 位的 PCMCIA，另一类是 32 位的 CardBus，支持 CardBus 的网卡最大吞吐量接近 90Mbps，是目前主流的在售笔记本电脑网卡。

3. 服务器网卡

去过机房的朋友都知道，服务器在正常工作的时候，一般只接电源线和网线两根线。显示器、键盘、鼠标这些在服务器中属于备用配件，只有在安装系统、进行大的系统调试时才用得上。平时服务器在工作的时候，对其进行的控制和调配，都是通过网络进行远程控制完成的。所以，网卡对于服务器来说是必不可少的一个部件。

服务器网卡是网卡里面最贵的，价格从千元左右到几万元的都有，常见的服务器网卡芯片厂商，有 Intel、3COM、Marvell、Broadcom 等，对于这些品牌的网卡，几百元的只能算是入门级的，几千元的网卡也很常见。服务器网卡的数据传输速度一般为千兆，目前也有一部分服务器安装了万兆网卡。服务器网卡与普通计算机网卡的区别在于：普通计算机的网卡主要是将计算机和局域网相连接，而服务器网卡则是用于将服务器和交换机等网络设备进行连接。

第二章 网络设备认知



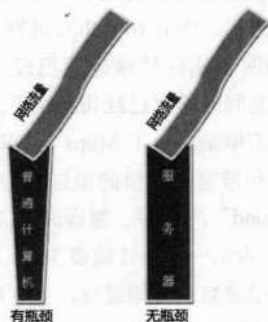
高价的服务器网卡

在服务器中使用网卡，有几个与普通计算机使用的网卡不同的特点：

一是网卡数量多。普通计算机一般情况下只要一块网卡就足够了，而服务器一般需要两块或更多的网卡。

二是数据传输速度快。服务器的访问流量一天有个上万次是不足为奇的，所以，服务器的网卡必须能够承载大数据流量。因此，目前的服务器一般都是使用千兆网卡，也有一些是使用了万兆网卡，这样才能提供高速的网络传输能力。

如果把整个计算机系统当作一个城市的话，网卡就是港口，主板上的总线则是港口配套的道路。普通计算机上的千兆网卡，就好像道路很小的港口，虽然港口的入口很大，但是里面配套的道路却很小，进来的货物根本不能及时的运走。



总线与瓶颈

所以，普通计算机上的千兆网卡，多数情况下根本达不到真正的千兆网卡的速度。而服务器的网卡，则从入口到出口都具备巨大的带宽，所以能达到真正的千兆速度。

三是 CPU 占用率低。由于服务器的 CPU 会不停地处理大量的数据，所以，网卡对 CPU 的占用率要低，以便节省出相应的资源用于对其它数

据进行处理。所以，服务器专用网卡都具有特殊的网络控制芯片（有的网卡还集成了处理器和内存），它可以从主 CPU 中接管许多网络任务，使主 CPU 能够集中“精力”运行网络操作和应用程序，大大减轻 CPU 的负担。

四是安全性能高。许多服务器网卡具有容错功能，如采用 Adapter Fault tolerance (AFT，网卡出错冗余)、Adapter Load Balancing (ALB，网卡负载均衡)、Fast Ether Channel (FEC，快速以太网通道) 等技术。

所谓 AFT 技术，是指在服务器上安装两块网卡，一块为主网卡，另一块作为备用网卡，然后用两根网线将两块网卡都连到交换机上。在服务器和交换机等网络设备之间建立主连接和备用连接。一旦主连接因为数据线损坏或网络传输中断导致连接失败，备用连接会在几秒钟内自动顶替主连接的工作，通常网络用户不会觉察到任何变化。这样一来就避免了因一条线路发生故障而造成整个网络瘫痪，可以极大地提高网络的安全性和可靠性。

所谓 ALB 技术，是指在多块网卡之间通过平衡数据流量的方法来增加吞吐量，每增加一块网卡，就可以增宽到更高的通道。另外，ALB 还具有 AFT 同样的容错功能，一旦其中一条链路失效，其他链路仍可保障网络的连接。当服务器网卡成为网络瓶颈时，ALB 技术无须划分网段，网络管理员只需在服务器上安装两块具有 ALB 功能的网卡，并把它们配置成 ALB 状态，便可迅速、简便地解决瓶颈问题。

所谓 FEC 技术，是 Cisco 公司针对 Web 浏览及 Intranet 等对吞吐量要求较大的应用而开发的一种增大带宽的技术。FEC 同时也为进行重要应用的客户 / 服务器网络提供高可靠性和高速度。

4. 无线网卡

无线网卡的作用类似于以太网中的网卡，作为无线网络的接口，实现计算机与无线网络的连接。无线网卡根据接口类型的不同，主要分为三种类型，即 PCMCIA 无线网卡、PCI 无线网卡和 USB 无线网卡。



PCMCIA 无线网卡仅适用于笔记本电脑，支持热插拔，可以非常方便地实现移动式无线接入。



PCMCIA无线网卡

PCI 接口无线网卡适用于普通的台式计算机使用，除了安装有些不便外，信号强度还是不错的。



PCI接口无线网卡

USB 接口无线网卡适用于笔记本电脑和台式机，支持热插拔。USB 网卡呈现越来越小巧的趋势，因此携带和使用起来都很方便。



USB无线网卡

USB 无线网卡的接口类型一般为 USB 2.0，有效工作距离为：室内最远 100 米，室外最远 300 米，当然这个距离会因实际环境而异。

2.1.2 网卡的选购

网卡是计算机与外部网络连接的桥梁，所以它的性能将会影响到计算机网络的性能。网卡的

选购比较简单，主要需要注意如下几个方面：

一是选择性价比高的网卡。在选购网卡时，如果普通品牌网卡的价格和品牌网卡的价格相关不多（如 5~15 元），那么建议选择品牌网卡。



TP-LINK品牌标志

因为过硬的品牌往往代表着过硬的质量和优质的售后服务。常见的网卡名牌有：Intel、TP-LINK、D-Link、阿尔法、Netcore、腾达、NETGEAR、3COM 等等。

虽然网卡属于技术含量比较低的产品，但是对制作工艺等方面仍然有着严格的要求。有的网卡安装、使用都没有什么问题，但使用时间一长就会导致系统频繁死机等问题出现，就是因为做工、用料方面不足导致的。

二是根据需求选择合适的网络传输速度。对于家庭用户来说，使用 100Mbps 的网卡就可以了，因为这样的网卡实际传输速度已经达到 10MB/S 左右，数据复制的速度已经相当快了。

这里要简单解释一下 Mbps 与 MByte 的区别，在网络设备和带宽中使用的单位均为 bps。bps 是“Bit Per Second”的缩写，翻译成中文就是比特位每秒，也就是表示一秒钟传输多少位 (Bit) 的意思，此缩写用来描述数据传输速度。如，Mbps 就表示了每秒传输 1,000,000 比特 (bit)，4Mbps= 每秒钟传输 4M 比特。

再来说说 MByte 的含义，由于 1Byte (字节) = 8bit，所以 1MByte 实际上就等于 8MBbps。以 100Mbps 的网卡为例，其每秒传输的速度为：100Mbps/8=12.5MByte/s，也就是 10MB 左右每秒。

对于局域网传输量很大的企业网络或服务器来说，一般需要使用 1000Mbps 的网卡，并且为网卡配备相应速率的网络交换设备，否则网络的

第二章 网络设备认知

传输速度就会出现“瓶颈”问题。

2.1.3 网卡的安装

因为在硬件安装方面不需要做任何设置，所以网卡的安装非常简单。具体的步骤如下：

STEP 1 拆开机箱，并使用螺丝刀将机箱后部挡片上的螺丝钉拧下。拧下螺丝钉后，用手将挡片从机箱上取出。

STEP 2 将网卡从防静电袋中取出，用双手分别捏住网卡的两端，对着 PCI 插槽垂直插入插槽中，并均匀用力地往下按。



安装网卡

STEP 3 网卡的接口插脚完全插入 PCI 槽后，将挡板上的螺丝孔位置对准机箱上的螺丝孔位置，用螺丝钉将网卡固定在机箱中，以免网卡松动。

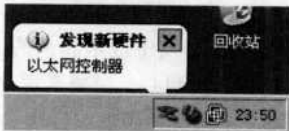


注意

如果可能的话，尽量选择将网卡的插槽位置远离其它板卡（如声卡或显卡），这样可以尽量减少彼此之间的干扰。

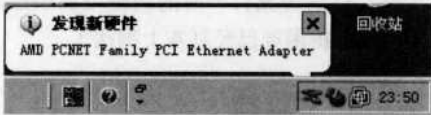
完成了硬件的安装后，将制作完成的网线一端的水晶头插入网卡的 RJ45 插槽中即可。

STEP 4 按电脑主机上的电源开关打开电脑，在进入 Windows 的桌面环境后，系统将会提示“发现新硬件”。



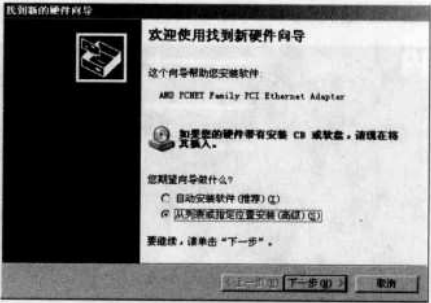
发现新硬件

STEP 5 由于 Windows 2000/XP/2003 等系统可以自动识别并支持即插即用的硬件，所以通常能够立刻识别出新安装的网卡型号。



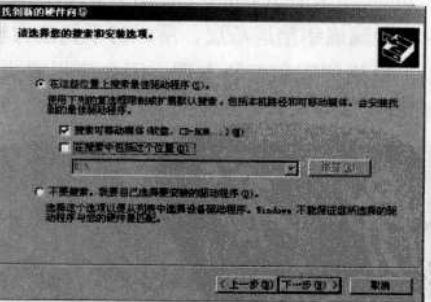
识别出网卡的型号

STEP 6 如果网卡可以使用系统内置驱动程序中的驱动，那么系统会自动安装好它的驱动，并使其处于硬件安装完成状态。否则，会自动弹出如图所示的向导窗口，选中“从列表或指定位置安装（高级）”项并单击“下一步”按钮继续。



安装新硬件向导

STEP 7 在弹出的如图所示窗口中，将随网卡附送的驱动光盘放入光驱。单击“下一步”按钮后，会自动搜索到相应的驱动程序。



指定驱动所在位置

STEP 8 单击“下一步”按钮后，安装向导就会开始安装该驱动程序。完成后，根据提示重新启动电脑即可。

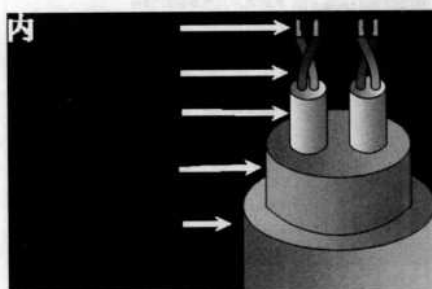


2.2 传输介质

目前，最常用的传输介质是双绞线、光纤和无线传输。以前曾流行一时的同轴电缆虽然成本低，但由于维护困难已经基本上淘汰了。

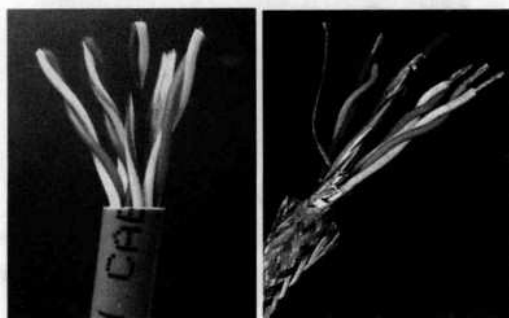
2.2.1 双绞线

双绞线（Twisted Pair）是目前使用率最高的网络数据传输介质，由两根 22-26 号具有绝缘保护层的铜导线组成，并按照一定的密度互相绞在一起，以便降低杂音（Noise）和串音（Crosstalk）等干扰，因为每一根导线在传输中辐射的电波会被另一根导线上的发出的电波抵消。在我们购买的网线中，这样的线共有 4 对 8 芯（即 8 根线缆）。



STP型双绞线的结构

双绞线依其组成方式可分为“无屏蔽双绞线”（Unshielded Twisted Pair）（左图）和屏蔽式双绞线（Shielded Twisted Pair）（右图）两种。前者由于少了金属或铝箔屏蔽层，所以防干扰能力较差，但由于价格便宜和安装方便，因此使用率反而比后者较广。



两种双绞线

根据最大传输率的不同，双绞线分为三类、五类、超五类和六类几种，即：

- > 三类的速率为 10Mit/s；
- > 五类的速率为 100Mit/s；
- > 超五类的速率为 155Mit/s；
- > 六类的速率为 1000Mit/s；

每条双绞线的最大传输距离为 100M（米），如果要加大传输距离，需要在两段双绞线之间可安装如图所示的中继器（又叫网络延长器），最多可安装 4 个中继器。如安装 4 个中继器连接 5 个网段，则最大传输距离可达 500M。



中继器

和双绞线配套使用的是 RJ45 水晶头。水晶头也有超五类、超五类屏蔽、六类（千兆）、六类屏蔽等区别，选购的时候要注意这一点。

要将双绞线与水晶头连接到一起，需要借助网线钳来完成这项任务。网线钳从十几元到一、二百元都有，其主要区别在于有的只能做网线接头，有的能同时做电话线接头，以及刀口的用料不同等等。



网线钳

使用网线钳将网线压进水晶头的方法十分简单，但整个过程需要耐心，简要实现方法如下：

STEP 1 左手紧握住距离双绞线头的 2CM 处，用网线钳把这 2CM 外皮旋转割去并切断，把八根

第二章 网络设备认知

线缆理开、拉直（由于线缆相互缠绕着，因此线缆会有一些的弯曲，需要把线缆尽量扯直）。



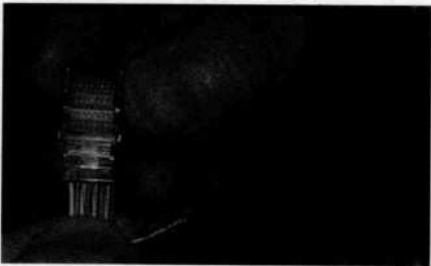
理开、拉直网线

STEP 2 按白橙（和橙是一组）、橙、白绿、蓝、白蓝、绿、白棕、棕的顺序（双绞线的制作方式有两种国际标准，分别为 EIA/TIA568A 以及 EIA/TIA568B，这个顺序为后者）理好，露出图示的部分并切齐，线头与外皮的距离为 1CM 左右。



把线头切齐

STEP 3 用左手捏住剪齐的线头，用右手将水晶头套在线头上。水晶头凹槽内的金属触点共有 8 个，简称“8C”（Contact，触点），特别需要注意的是水晶头的引脚序号，当金属片面对我们的时候从左至右引脚序号是 1-8，序号对于网络连线非常重要，不能搞错。



把水晶头套好

STEP 4 右手捏住水晶头不放，左手把线头向水晶头内推进，直至能在水晶头的头部看到 8 根线头的铜芯。



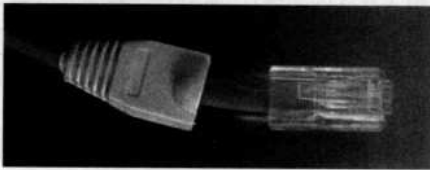
线头抵到水晶头的头部

STEP 5 将水晶头放入压线钳的压线口，用劲握压线钳手柄几次。这样，就可以把网线和水晶头连接到一起了。



将网线与水晶头压好

最后，已经将网线与水晶头压好的效果如图所示，在有的网线上还会添加水晶头护套，可以有效避免水晶头的卡子（定位压片）被折断。



制作完成的水晶头

压好的网线一般需要测试一下是否通，也就是两端的 8 根线是否分别压到位。测试的方法有两种，一是将网线插到两台电脑中；二是使用测线仪进行测量。



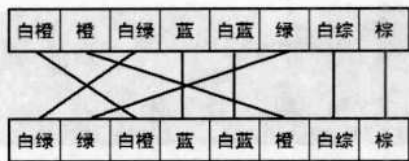
使用测线仪测试

在测试网线的时候，网线的两端必须同时插入测线仪的两个接口中。在按下测试开关后，测线仪的两个部分从 1 到 8 的灯都要同步闪动，这



样才能表示网线与水晶头已经制作成功。

双绞线的连接方法主要有两种，分别为直通线缆以及交叉线缆。简单地说，直通线缆就是水晶头两端都同时采用 T568A 标准或者 T568B 的接法，而交叉线缆则是水晶头一端采用 T586A 的标准制作，而另一端则采用 T568B 标准制作，即 A 水晶头的 1、2 对应 B 水晶头的 3、6，而 A 水晶头的 3、6 对应 B 水晶头的 1、2。



交叉线缆的做法

若测试的线缆为交叉线缆（见本书组建家庭局域网部分的连接方法示意图），其中一侧同样是依次由 1～8 闪动绿灯，而另外一侧则会根据 3、6、1、4、5、2、7、8 这样的顺序闪动绿灯。若出现任何一个灯为红灯、黄灯或者不亮，都证明存在断路或者接触不良现象，此时最好先对两端水晶头再用网线钳压一次，再测，如果故障依旧，再检查一下两端芯线的排列顺序是否一样，如果不一样，随便剪掉一端重新按另一端芯线排列顺序制做水晶头。直到测试全为绿色指示灯闪过为止。

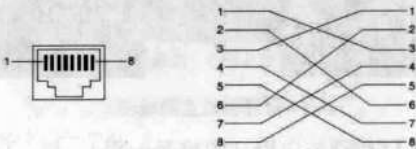
在什么情况该做成直通线缆？交叉线缆又该用在什么场合呢？下面，在如表 2-1 所示中给出了相应的答案供读者们参考。

表2-1

设备连接	使用线缆
计算机连接计算机	交叉
计算机连接集线器	直通
集线器连接集线器（普通口）	交叉
集线器连接集线器（级联口to级联口）	交叉
集线器连接集线器（普通口to级联口）	直通
集线器与交换机	交叉
集线器（级联口）与交换机	直通
交换机与交换机	交叉
交换机与路由器	直通
路由器与路由器	交叉

最后，要提醒读者们注意：千兆网线和百兆网线的制作区别是：百兆网络只需使用 1、2、3、6 四根线进行数据传输的，这就是为什么有些网

卡插槽只有 4 根铜芯的原因。而千兆网络是需要 8 根线进行数据传输的，所以，千兆网线的制作方法是：1 对 3、2 对 6、3 对 1、4 对 7、5 对 8、6 对 2、7 对 4、8 对 5。



千兆网线制作示意图

从网线颜色标识连接的话，颜色连接如下：

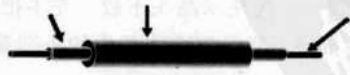
- 1、橙 对 白绿
- 2、白橙 对 绿
- 3、白绿 对 白橙
- 4、蓝 对 白棕
- 5、白蓝 对 棕
- 6、绿 对 橙
- 7、白棕 对 蓝
- 8、棕 对 白蓝

百兆网线的 8 根线缆每根都是一根铜丝，而千兆网线的 8 根线缆的每根是由多根镀银线或更细的多股铜线组成，进而确保了传输效率，且更不容易被折断。

2.2.2 光纤

所谓光纤（Fiber-optic）就是纤维状的光导体，可用来架设传输线路。光纤的优势是不会辐射电子信号，所以光纤网络无论在性能还安全性方面，都相对于使用双绞线的网络有着很大的进步。光纤支持的传输距离高达 2KM（公里）以上，是目前组建较大规模局域网的必选传输介质。

光纤仅受光电转换器件的限制，其传输速率高达 100GB/S，即接近光速。光纤有单芯和多芯两种，单芯一共包含三层，即玻璃内芯、玻璃封套和塑料外套。



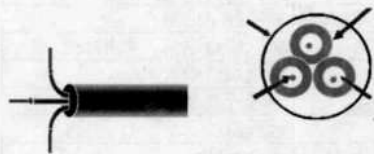
单芯光纤的组成

玻璃内芯位于光纤的最中央，是真正传送光

第二章 网络设备认知

脉冲信号的媒介，材质主要是以玻璃为主。封套也以玻璃制成，主要作用是让光线射入光纤核心时，可以透过这层产生反射，以确保光线能前进抵达接收端。外套位于光纤的最外层，主要是用来保护光纤，并且减少因折射而损失的光能。

多芯光纤的组成相对于单芯光纤来说，只是多了几条玻璃内芯而已。



多芯光纤的组成

由于光线在光纤中的传送方式不同，光纤可以分为单模（Single Mode）和多模（Multimode）两种不同的类型，所谓“模”就是指以一定的角度进入光纤的一束光线，单模光纤使用的是激光二极管（LD）作为发光设备，多模光纤使用的是发光二极管（LED）作为发光设备，如图 2-34 所示。光纤的传输原理：利用了光的反射。



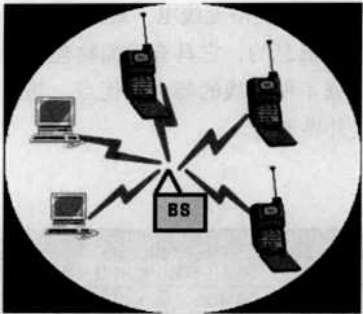
单模和多模

多模光纤一般被用于同一办公楼或距离较短的区域内架设局域网时使用，单模光纤通常被用于连接办公楼之间或在较大的区域内架设局域网时使用。

2.2.3 无线传输

无线传输是近年来的热门话题，这几年生产的笔记本电脑几乎都配备了无线模块。借助无线技术，无论在何时（Whenever）、何地（Wherever），人们都能进行网络构建！

很多人都觉得来无影去无踪的无线传输很神秘，其实，我们很久以前就在和无线通信打交道了，如使用寻呼机、手机时都需要使用无线数据传输。



基站覆盖的无线电区域

很多人使用卫星接收方法收看电视节目，很明显，电视节目的数据也是使用无线方法传输的。



卫星也使用无线传输

在 1895 年意大利的 G·马可尼利用电火花产生的电磁波，并先后在 9m、975m 和 3000m 的地方收到电报信号后，从此开辟了无线通信的先河。在第二次世界大战期间，当时美国陆军采用无线电信号进行资料传输。他们研发出了一套无线电传输科技，并且采用相当高强度的加密技术。当初美军和盟军都广泛使用这项技术。这项技术让许多学者得到了灵感，在 1971 年时，夏威夷大学（University of Hawaii）的研究员创造了第一个基于封包式技术的无线电通讯网络，这被称作 ALOHNET 的网络，可以算是相当早期的无线局域网（WLAN）。这最早的 WLAN 包括了 7 台计算机，它们采用双向星型拓扑（bi-directional star topology），横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛（Oahu Island）上。从这时开始，无线网络可说是正式诞生了。



无线传输是使用无线电、短波、微波、卫星、光波等携带信息的，它具有无需物理连接、适用于长距离或不便布线的场合等优点，其最大不足就是易受外界干扰。

利用无线通信，可以传送电报、电话、传真、数据、图像以及广播和电视节目等通信业务。

在如表 2-2 所示中，对常用传输媒体进行了传输速率、性能、价格等多方面的比较。

表2-2

传输媒体	速率	传输距离	性能(抗干扰性)	价格	应用
双绞线	10-1000Mb/s	几十KM	可以	低	模拟/数字传输
50Ω同轴电缆	10Mb/s	3KM内	较好	略高于双绞线	基带数字信号
75Ω同轴电缆	300-450MHz	100KM	较好	较高	模拟传输电视、数据及音频
光纤	几十Gbps	20KM	很好	较高	远距离传输
短波	<50MHz	全球	较差	较低	远程低速通信
地面微波接力	4-6GHz	几百KM	好	中等	远程通信
卫星	500MHz	18000KM	很好	与距离无关	远程通信

目前，市场上比较常见的无线传输介质有无线局域网 (WLAN)、蓝牙 (Bluetooth)、IrDA (红外线数据)、HomeRF、无线微波接入技术、GPRS/CDMA 无线接入等等。在本书中，无线技术的应用主要使用了无线局域网、蓝牙、红外线几个方面。其中，无线局网络目前主要应用于家庭或中小型办公网络中，它的网格标准都是使用 802.11 系列，并进行了如表所示的细分。标准的细分除了对传输速度加以区分外，更重要的是对安全方面加以了改进。

表2-3

标准	描述
802.11	定义了无线网络传输概念的基准规范，即频率2.45GHz，传输速度为1~2Mbps
802.11a	传输速度增加到54 Mbps
802.11b	增加传输速度，传输范围较好，但容易受到无线信号的干扰，只能使用11Mbps
802.11g	使用54 Mbps，范围比802.11b要窄，是目前使用最多的协议版本
802.11i	为无线网络建立了认证和加密处理的标准，并保证完整性

1997 年 IEEE 制订出无线局域网的协议标准的第一部分：802.11。在 1999 年又制订了 802.11b 和 802.11a 两部分。先推出的 IEEE802.11b 工作于 2.4GHz 频带，物理层支持 5.5 Mbps 和 11 Mbps 两种速率。它的传输速率可因环境干扰或传输距离而变化，在 11 Mbps、5.5 Mbps、2 Mbps、1 Mbps 之间切换，而且在 2 Mbps、1 Mbps 速率时

与 IEEE802.11 兼容。

后推出的 IEEE802.11a 工作于 5GHz 频带，物理层速率可达 54Mbps，基本满足了现行局域网绝大多数应用的速度要求，而且采用了更为精密的算法。但是，IEEE802.11a 芯片价格昂贵，而且与 IEEE802.11b 标准不兼容，因此正逐渐淡出人们的视野。

其次推出的 IEEE802.11g 也工作于 2.4GHz 的频带，物理层速率可达 54Mbps~108Mbps，并完全兼容于 IEEE802.11b 标准，可与原有的 IEEE802.11b 产品实现正常通讯。现在，大多数厂商生产的无线局域网产品都基于 802.11G 标准。

未来将要使用的 IEEE802.11n 让人期待，百兆有线网络的传输吞吐率一般可达 80Mbps，而 802.11n 的传输吞吐率最低都可达到 90 Mbps，已完全超过百兆有线网络。并且具有更大的覆盖范围，实现了高带宽、高质量的无线网络服务，显示出其巨大的发展潜力。作为新一代的无线传输标准协议，在传输速率方面，802.11n 可以将无线网络传输速率由 802.11a、802.11b 及 802.11g 提供的 54M、108M，提高到 300M 甚至 600M。

与其它网络设备基本相同，无线局域网设备也大致分为三大阵营：

第一阵营是美国产品，如 AVAYA、CISCO、3COM 等，品质优良、工作稳定、性能出众、管理方便，但价格居高不下，普通用户很难承受。

第二章 网络设备认知

第二阵营是台湾地区产品，如 D-LINK、ACCTON 等，作为美国公司的 OEM 厂商，制作工艺自然无话可说，产品性能也相当不错，具有非常高的性能价格比。

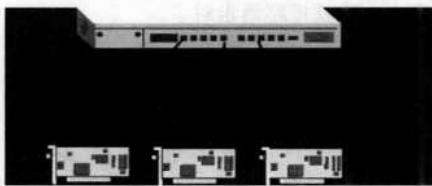
第三阵营是大陆产品，如神州数码、清华比威、TP-LINK 等，产品质量也不错，价格也很便宜，最适合小型办公网络使用。

2.3 网络交换设备

如果说各类计算机是机动车、非机动车和行人，网线是马路，那么网络交换设备就是十字路口。它连接了各条马路（网线）供车辆与行人通行。有的交换设备还具有网管等功能，就相当于有的十字路口配备了交通警察指挥交通一样。在星形拓扑结构的网络中，网络交换设备是不可或缺的构件。

2.3.1 集线器

集线器（HUB）是工作在物理层的网络设备，通过本书前面的内容，我们知道：物理层确定了电缆与网卡的连接方式，以及发送数据时使用的传输技术，在此层上传输的数据是无结构的原始数据。也就是说，它用于识别网卡的硬件设置并与之进行配合。集线器的主要功能除了可以对源计算机发送的数据进行接收和转发外，还能够起到放大信号、扩大网络距离等作用。



集线器的工作方式

由于集线器的功能简单，加之交换机、路由器的性价比越来越高，目前局域网组建中基本上已经不使用集线器作为中央节点设备了。鉴于此，用户只需对集线器有个大致的认识就可以了。

集线器按传输速率划分，可以分为 10Mbps 和 100Mbps 两种；按端口类型可以分为 RJ45 和 USB 两种，如图所示是常见的 RJ45 集线器。



集线器

在这类设备上一般有两种接口，一是 Uplink 接口，用于连接 ADSL、集线器、交换机等上层网络设备。二是 RJ45 接口，用于连接计算机或其它设备。通过 USB 接口集线器，可以将计算机、打印机等设备添加网络中。



集线器端口的使用



USB集线器

在局域网中按集线器工作原理的不同，大致分为共享式集线器和交换式集线器两种。

共享式集线器不能提高网络性能，也不能检测信号错误，它们只是简单地从一个端口接收数据并通过所有端口分发。作为星型拓扑以太网入门级设备，共享式集线器的总带宽将被连接的设备平分，例如集线器的总带宽为 10Mbps/S，当连接了 4 台计算机并同时上网时，每台工作站的



平均带宽仅为 2.5 Mbps/S。

交换式集线器与共享式集线器不同，它具有信号过滤的功能。它可以只将信号传送给某一已知地址的端口，而不像共享式集线器那样将信号传送给网络上的所有端口，这样就会产生大量的垃圾数据（产生网络风暴）让带宽利用率降低。

除此之外，交换式集线器上的每一个端口都是拥有专用带宽的，它可以让多个端口之间同时进行对话，而不会互相影响。交换式集线器可以直通传送、存储转发和改进型直通传送来传送数据，其工作效率大大高于共享式集线器。这种集线器和交换机之间的特性几乎没区别。

目前，集线器的品牌厂商有：D-Link、阿尔法、3Com、AVANET、Netcore 等，价格从几十元到上千元不等。由于各个厂家的集线器产品性能差无几，一般情况下没有必要去花钱买高端的。

2.3.2 交换机

当前的组网环境里面，交换机（Switch）是使用最多的网络交换设备。1993 年，局域网交换设备出现，1994 年在我国掀起了交换网络技术的热潮。至今，交换机无论在硬件或软件方面，都已经有了长足的进步。

“交换”是指按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术统称。广义的“交换机”是指一种在通信系统中完成信息交换功能的设备。

1. 交换机原理概述

很多老电影中都可以看到这样的镜头：电话旁的 A 用户拿起话筒后，一阵猛摇旁边的摇把，立即话务小姐就会接到这个要求通话的信号，听到 A 用户要求与谁进行通话的请求后，她会立刻把线头插在相应的出口，为两个用户端建立起通话连接，直到通话结束再拔下。这个过程就是通过人工方式建立起来的交换技术，当然现在早已普及了程控交换机，交换的过程都是自动完成的。

举这个例子是为了说明交换机的作用相当于这个话务小姐。交换机在接收到某个端口的信号

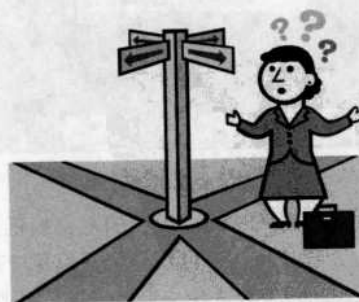
后，它也会立即将来源端口与目的端口连接起来。



交换机

交换机与集线器的工作原理有本质的不同，集线器在接收到来自某个端口的数据后，会将接收到的数据进行还原并在所有端口进行发送，它既不检测数据类型和校验是否正确，也不确定目的地址。而交换机则可以通过自学习（如同话务小姐记姓名与号码的关系）功能，把所有端口的 MAC 地址和对应的 IP 地址记忆下来，并直接把数据送到相应的目的端口，大大降低了网络风暴的产生和增加了网络带宽的利用率。当然，如果目的端口的 MAC 地址在内存中没有的话，交换机也会广播到所有的端口，在接收端口回应后交换机会“学习”新的地址，并把它添加入内部地址表中。

在计算机网络系统中，交换概念的提出是对于共享工作模式的改进。形象的说就比如一条路前面有 N 个分叉，集线器就相当于每条路都走一遍直到你走对为止，而交换机可以直接选择正确的分叉，一次就把路给走对了。



交换机的效果更好

实际上，交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有端口都挂接在这条背部总线上，控制电路收到数据包以后，处

第二章 网络设备认知

理端口会查找内存中的地址对照表以确定目的 MAC（网卡的硬件地址）的 NIC（网卡）挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口。总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。

目前，交换机在交换技术上主要是使用“帧交换”技术，它通过对传统传输媒介进行微分段，提供并行传送的机制。这样可以减小冲突域，以获得高的带宽。通常，对帧的处理方式有如下几种：

一种是直接交换。提供快速处理能力，只读出网络帧的前 14 个字节，便将网络帧传送到相应的端口上。由于不需要存储，所以延迟非常小，交换非常快，这是它的优点。它的缺点是，因为数据包内容并没有被以太网交换机保存下来，所以无法检查所传送的数据包是否有误，不能提供错误检测能力。由于没有缓存，不能将具有不同速率的输入/输出端口直接接通，而且容易丢包。

第二种是存储转发。存储转发方式是计算机网络领域应用最为广泛的方式。它把输入端口的数据包先存储起来，然后进行 CRC（循环冗余码校验）检查，在对错误包处理后才取出数据包的目的地址，通过查找表转换成输出端口送出包。正因如此，交换速度会相对前一种略慢。但是它可以对进入交换机的数据包进行错误检测，有效地改善网络性能。尤其重要的是它可以支持不同速度的端口间的转换，保持高速端口与低速端口间的协同工作。

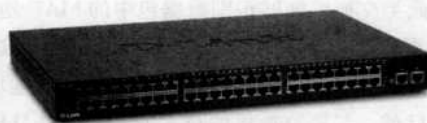
第三种是碎片隔离。这是介于前两者之间的一种解决方案。它检查数据包的长度是否够 64 个字节，如果小于 64 字节说明是假包并丢弃该包；如果大于 64 字节则发送该包。这种方式也不提供数据校验。它的数据处理速度比存储转发方式快，但比直通式慢。

2. 交换机的分类

作为局域网的主要连接设备，以太网交换机成为应用普及最快的网络设备之一。随着交换技术的不断发展，交换机的价格急剧下降，这直接导致了集线器的快速出局。

从广义上来看，交换机分为两种：广域网交换机和局域网交换机。广域网交换机主要应用于电信领域，提供通信的基础平台。而局域网交换机则应用于局域网络，用于连接终端设备，如 PC 机及网络打印机等。

从传输介质和传输速度上可分为以太网交换机、快速以太网交换机、百兆/千兆/万兆以太网交换机，以及 FDDI 交换机、ATM 交换机和令牌环交换机等。



D-Link 48口百兆+2口千兆交换机

从规模应用上又可分为企业级交换机、部门级交换机和工作组交换机等。



机架式交换机

各厂商划分的尺度并不是完全一致的，一般来讲，企业级交换机都是机架式，部门级交换机可以是机架式（插槽数较少），也可以是固定配置式，而工作组级交换机为固定配置式（功能较为简单）。另一方面，从应用的规模来看，作为骨干交换机时，支持 500 个信息点以上大型企业应用的交换机为企业级交换机，支持 300 个信息点以下中型企业的交换机为部门级交换机，而支持 100 个信息点以内的交换机为工作组级交换机。

根据工作协议层进行分类的话，交换机可以分为二、三、四层交换机。对应层次越高，说明交换机的技术含量越高。限于本书内容只涉及到二、三层交换机，下面仅对这两种交换机进行介绍。

(1) 二层交换机

众所周知，交换机工作在 OSI 参考模型第二层：数据链路层上，主要功能包括物理编址、网络拓扑结构、错误校验、帧序列以及流量控制等等。

* 物理编址（相对应的是网络编址）定义了设备在数据链路层的编址方式。



* 网络拓扑结构包括数据链路层的说明，定义了设备的物理连接方式，如星型拓扑结构或总线拓扑结构等。

* 错误校验向发生传输错误的上层协议告警。

* 数据帧序列重新整理，并传输除序列以外的帧。

* 流量控制可以延缓数据的传输能力，以使接收设备不会因为在一时刻接收到了超过其处理能力的信息流而崩溃。

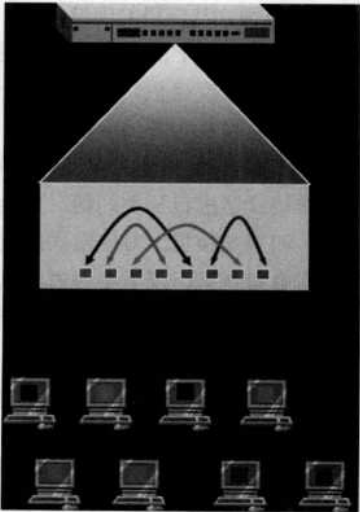
此类交换机能够识别数据包中的 MAC 地址，并根据这个地址进行数据的转发，然后将这些 MAC 地址与对应的端口记录在自身的一个地址表中。目前，二层交换机的技术非常成熟并且价格低廉，已经成为当前使用量最大的交换机设备。

二层交换机的具体工作流程如下：

STEP1 当交换机从某个端口收到一个数据包，它先读取包头中的源 MAC 地址，这样它就知道源 MAC 地址的机器是连在哪个端口上的。

STEP2 读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

STEP3 如果表中有与目的地 MAC 地址对应的端口，把数据包直接复制到这个端口上。此时，交换机可以建立多个并发的通信，如 8 个端口可建立 4 个并发通信。

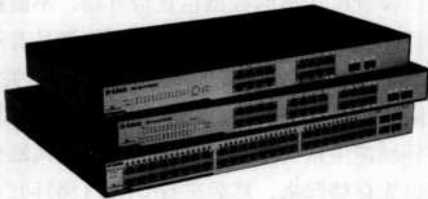


建立多个并发通信

STEP4 如果表中找不到相应的端口则把数据包广播到所有端口上，当目的机器对源机器回应时，交换机又可以学习到目的 MAC 地址与哪个端口对应，在下次传送数据时就不再需要对所有端口进行广播了。不断的循环这个过程，对于全网的 MAC 地址信息就都可以学习到，二层交换机就是这样建立和维护它自己的地址表。

(2) 三层交换机

由于网络的第三层（即网络层）支持网络路由，所以三层交换机也提供了路由管理功能，具有部分原来独属于路由器的“路由”功能。它可以将 IP 地址信息进行分析并进行路径选择，从而实现了不同网段间的数据交换。大多数三层交换机采用了灵活的模块化结构，有利于功能扩展和调整。规模较大的网络中三层交换机已成为基本配置。



高性能交换机

三层交换机的具体工作流程如下：

以 A 计算机向 B 计算机发送数据为例，在已知 B 计算机 IP 地址的前提下。A 会用子网掩码取得网络地址，判断 B 的 IP 是否与自己在同一网段。如果在同一网段，但不知道转发数据所需的 MAC 地址，A 就发送一个 ARP 请求，B 返回其 MAC 地址。



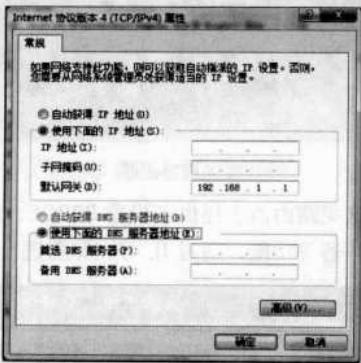
使用ARP命令

A 用此 MAC 地址封装数据包并发送给交换机，交换机起用二层交换模块，查找 MAC 地址表，

第二章 网络设备认知

将数据包转发到相应的端口。

如果 B 的 IP 地址显示不是同一网段的，并且在缓存条目中没有对应的 MAC 地址条目，那么，就需要将第一个正常数据包发送向一个缺省网关，这个缺省网关一般在操作系统中已经设好。



设置默认网关

当三层模块接收到此数据包时，会查询路由表以确定到达 B 的路由是什么。此时，会将缺省网关的 MAC 地址设置为源 MAC 地址，以主机 B 的 MAC 地址为目的 MAC 地址。然后，确立 A 与 B 的 MAC 地址以及转发端口的对应关系，并记录进缓存条目表，以后的 A 到 B 的数据，就直接交由二层交换模块完成。

其实，三层交换机的最重要的功能是加快大型局域网络内部的数据的快速转发，加入路由功能也是为这个目的服务的。

3. 交换机的管理功能

交换机可以分为网管型和非网管型的，所谓网管型就是提供了一个管理界面，可以通过软件方式对交换机进行配置。

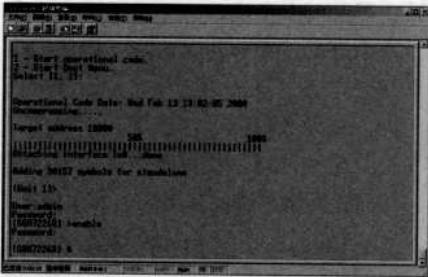
网管型交换机可以通过以下几种途径管理：通过 RS-232 串行口（或并行口）管理，或者通过 IE 等浏览器管理和通过网络管理软件管理。

网管型交换机通常会附带一条串口电缆，供交换机管理使用。先把串口电缆的一端插在交换机背面的串口里，另一端插在普通计算机串口里。



串口线

接着接通交换机和电脑电源，运行 Windows “超级终端”程序并按照交换机说明书设定好连接参数后，就可以通过串口电缆与交换机交互了。



登录交换机管理界面

这种管理方式下，交换机提供了菜单驱动的控制台界面或命令行界面。通过“Tab”键或箭头键在菜单和子菜单里移动，按回车键执行相应命令或使用专用的交换机管理命令集管理交换机。



注意

不同品牌的交换机命令集是不同的，甚至同一品牌的交换机，其命令也不同。使用菜单命令在操作上更加方便一些。

2.3.3 路由器

路由器（Router）是目前组网中最重要的网络交换设备之一，作为大型网络的核心构件，路由器和交换机一样是局域网和 Internet 网络的基础。路由器的主要任务是选择网络路径。

早在 40 多年之间就已经出现了对路由技术的

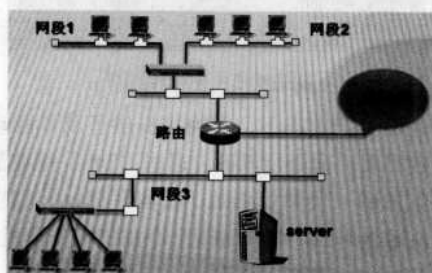


讨论，但是直到 80 年代路由技术才逐渐进入商业化的应用。路由技术之所以在问世之初没有被广泛使用，主要是因为 80 年代之前的网络结构都非常简单，路由技术没有用武之地。直到最近十几年，大规模的互联网络才逐渐流行起来，为路由技术的发展提供了良好的运行基础和平台。

1. 路由原理

路由是把信息从源穿网络传递到目的地的行为，在这个传递的过程中至少有一个中央节点。路由发生在第三层，即网络层。路由器利用网络层定义的“逻辑”上的网络地址（即 IP 地址）来区别不同的网络，进而实现网络的互连和隔离，并保持各个网络的独立性。

路由器上有多个端口，可以用于连接多个 IP 子网。路由器的一个作用是连通不同的网络，另一个作用是选择信息传送的线路。选择通畅、快捷的近路，能大大提高通信速度，减轻网络系统通信负荷，节约网络系统资源，提高网络系统畅通率，从而让网络系统发挥出更大的效益来。



使用路由器的拓扑

和集线器与交换机不同的是，路由器不广播消息，而是把广播消息限制在各自的网络内部，发送到其它网络的数据均先被送到路由器，再由路由器转发出去。路由器也有自己的缺省网关。

2. 路由的种类

目前，TCP/IP 网络全部是通过路由器互连起来，因特网就是成千上万个 IP 子网通过路由器连接起来的巨型网络。在不同的环境中，对路由器性能和功能方面的要求也是不同的，根据应用级别的不同，可以分为接入级路由器、企业级路由器、骨干级路由器等等。下面予以简单介绍。

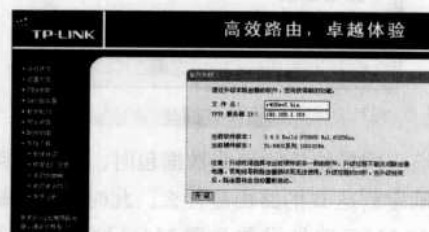
(1) 接入级路由器

接入级路由器用于连接家庭或小型企业客户，这类路由安装简单，支持和 ADSL 等网络设备共用。



接入级路由器

在这类路由器中提供了设置 PPPOE、防火墙、虚拟服务器等功能，通过 IE 等浏览器进行配置。



路由配置页面

通过此类路由，任何人都可以轻松实现 Internet 的共享，以及小型局域网的构建。

(2) 企业级路由器

企业级路由器除了可以连接多个逻辑上分开的网络外，还需要提供强大的安全功能。所谓的逻辑网络就是代表一个单独的网络或者一个子网。当数据从一个子网传输到另一个子网时，可通过路由器来完成。

针对不同的企业规模和网络需求，可以使用的路由器有：企业 VPN 路由器、企业高性能 VPN 路由器、企业单 WAN 口路由器、企业多 WAN 口路由器、企业模块化路由器等等。

如果从结构上对企业路由器进行划分的话，可以分为“模块化路由器”和“非模块化路由器”。模块化结构可以灵活地配置路由器，以适应企业不断增加的业务需求，非模块化的就只能提供固定的端口。通常中、高端路由器为模块化结构，低端路由器为非模块化结构。

企业路由器实际上就是一台计算机，因为它的硬件和计算机类似，路由器通常包括处理器

第二章 网络设备认知

(CPU)、用于存储信息的内存，主要用于连接外围设备或允许它和其它计算机通信各种端口，以及用于提供各种管理功能的操作系统。

企业路由器内置的软件有的运行在嵌入式操作系统上，有些运行在 UNIX 操作系统上……路由器软件一般能够实现路由协议、查表转发和管理维护等功能。由于因特网规模庞大，运行在因特网上路由器中的路由表非常巨大，可能包含几十万条路由。查表转发的工作可想而知非常繁重。在高端企业路由器中这些功能通常由 ASIC 芯片硬件实现。

目前，常用的企业路由器一般具有 3 层交换功能，提供千 / 万 Mbps 端口的速率、服务质量 (QoS)、多点广播、强大的 VPN、流量控制、支持 IPv6、组播以及 MPLS 等特性的支持能力，满足企业用户对安全性、稳定性、可靠性等要求。

(3) 骨干级路由器

骨干级路由器通常用于实现大型企业级的网络互联，工作在这个级别的路由器必须能够承受强大的数据吞吐量压力，速度和可靠性、安全性才是它最为人们所关注的，至于昂贵的价格就不足引以为奇了。



骨干级路由器

为了获得高度可靠性，骨干级路由器通常内置了热备份、双电源、双数据通路等传统冗余技术。此外，骨干 IP 路由器的主要性能瓶颈是在转发表中查找某个路由所耗的时间。当收到一个包时，输入端口在转发表中查找该包的目的地址以确定其目的端口，当包越短或者当包要发往许多目的端口时，势必增加路由查找的压力。因此，将一些经常访问的目的端口放到缓存 (Cache) 中能够提高路由查找的效率。

(4) 无线 AP 和路由

无线接入点或称无线 AP (Access Point)，其作用类似于以太网中的集线器。当网络中增加一个无线 AP 之后，即可成倍地扩展网络覆盖直径。

另外，也可使网络中容纳更多的网络设备。通常情况下，一个 AP 最多可以支持多达 80 台计算机的接入，当然，推荐数量为 30 台左右为宜。



无线 AP

无线 AP 都拥有一个或多个以太网接口，用于同时提供无线与有线的连接，可以将使用双绞线网卡的计算机与安装无线网卡的计算机连接在一起，从而实现无线与有线的无缝融合。另外，借助 AP 可接入固定网络的特性，还可以将分散布置在公司和家庭各处的无线 AP 利用双绞线连接在一起，实现类似于“小灵通”的无线漫游。

如果网络中原来拥有安装双绞线网卡的计算机，可以选择具备多个以太网接口的无线 AP，实现无线与有线的连接。否则，可以只选择拥有一个以太网端口的无线 AP，从而节约购置资金。

简单地说，无线路由就是在无线 AP 的基础上添加了路由功能，通过使用无线路由器可以实现无线局域网与广域网的连接。



无线路由

无线路由器通常还内置了防火墙、虚拟服务器等管理功能，用户可以通过 IE 浏览器实现 Web 式的管理。

第三章 操作系统的选择与安装

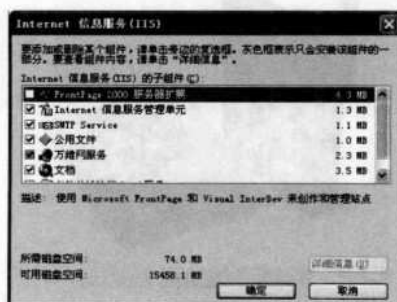
无论是什么样的网络，操作系统都是必不可少的。在不同的网络中，需要使用不同的操作系统（Operating System）来扮演不同的角色。比方说，在使用主从式拓扑结构的网络中，就需要在服务器里安装 Windows Server 2003/2008 或 Linux，在客户机里安装 Windows 2000 或 Windows XP（XP 是英文“eXPerience”（体验）的缩写）、Windows Vista。

不同的操作系统能够提供的功能不同，作为网络技术人员，不仅要熟悉这些操作系统的安装，还应能娴熟地运用这些操作系统中的网络功能，并在各类网络中实现各种各样的网络应用。

3.1 操作系统概述

没有安装操作系统的计算机是不具备任何功能的，只能被称为裸机。操作系统是计算机的灵魂所在，是用户和计算机沟通的接口。操作系统是所有软件中最重要的组成部分，它为软件与硬件之间“搭”起了一座交流的“桥”。越优秀的操作系统，“桥面”越宽敞，走得也就越舒服！

3.1.1 操作系统的分类



Windows XP网络服务组件列表

从网络这个角度来看，操作系统分为桌面级

和网络级两种操作系统。桌面级操作系统仅能够提供基本网络功能系统，如使用 IE 浏览器、收发邮件、建立受限制的各项网络服务（如网站、FTP）等。这样的操作系统有：Windows 9X、部分 Windows 2000 版本、Windows XP、Windows Vista 等。

所谓网络操作系统（NOS，Network Operating System）是针对网络环境专门开发的操作系统，提供了完整的网络服务，如网站、FTP、邮件、DNS……并且这些服务的使用没有任何限制，进而实现高效、可靠的网络通信能力。



服务器管理功能

第三章 操作系统的选择与安装

这样的操作系统有：Windows Server 2003/ 2008、Linux、Unix 等。

3.1.2 常见操作系统简介

目前，世界范围内能够开发出操作系统的软件厂商并不多，扳着手指头也能数得过来！但其中最为大家所熟悉、市场占有率最高的当属 Microsoft 公司设计的 Windows 系列操作系统！

1. Windows 98

作为曾经使用最为广泛的个人计算机操作系统，Windows 98 第一版和第二版几乎整整陪伴人们十年之久。其中，第二版的 Windows 98 SE 作为 Windows 9X 系列中最稳定的版本，它已经能够智能化地支持广泛的硬件设备（可以自动识别、安装部分品牌硬件的驱动）。

Windows 98 SE 的网络技术相对于以前的版本得到很大的改善，特别是其高效的“Internet 连接共享”功能，曾一度应用于家庭、网吧、企业等小型对等局域网，可谓是美名远扬。

2. Windows 2000

2000 年 2 月，微软发布了主要针对服务器用户的 Windows 2000（即 Windows NT 5.0）。



Windows 2000 共有 4 个版本，即：Windows 2000 Professional、Windows 2000 Server、Windows 2000 Advanced Server 和 Windows 2000 Data Server。其中，Windows 2000 Professional 是面向普通桌面用户设计的，而后面三者则是面向网络服务器设计的。

其中，Windows 2000 Professional 以其友好的操作界面，相对于 Windows 98 大幅度增强的各种特性得到了相当一部分人们的喜爱，这也使 Windows 2000 在普通用户心目中声名大震！在主从式局域网

中，这个版本常被安装到客户端计算机中。

3. Windows XP

2001 年，花费 10 亿美元、数千名软件设计师在汲取了 Windows ME 的失败教训和 Windows 2000 的成功经验后，开发的操作系统 Windows XP 诞生了！这款系统大大改善了人们对 Windows 家族“天生脆弱”的感觉！Windows XP 理所当然地得到了所有用户们的一致欢迎，并已经成为最引人注目的主流操作系统之一！

Windows XP 的全新设计、特别是 SP1、SP2、SP3 三个大型补丁包的推出，大大地改善了人们对 Windows 家族“体弱多病”的感觉。这使得 2001 年推出的 Windows XP 至今仍成为使用率最广的操作系统。

根据用户对象的不同，Windows XP 分为家庭版的 Windows XP Home Edition、办公扩展专业版的 Windows XP Professional、可以与 Tablet PC 完美结合的 Windows XP Tablet PC Edition、着重于智能化多媒体的操作系统 Windows XP Media Center Edition，以及用于支持 64 位处理器的 Windows XP Professional x64 Edition 等版本。

4. Windows Server 2003

2003 年 5 月 22 日，耗资 14 亿美元用于全球推广、被称为微软基于 .NET 平台“开山之作”的 Windows Server 2003 在中国如期发布。作为一款具有强大的集网络、安全、稳定等特性的操作系统，Windows Server 2003 主要面对网络服务器用户。



Windows Server 2003 是目前使用率最高的服务器系统，功能相当强大，性能也稳定，从诸多新增的组件可以看出微软在这款操作系统中倾注



了极多的心血。比方说它拥有价值数百万美元的安全机制，非常适用于高扩展性的应用程序需求，和对安全性能要求很高的服务器操作系统。

基于不同的用户需求和成本考虑，Windows Server 2003 提供了专门供网站服务的 Web Edition 版、供小型部门使用的 Standard Edition 版、可以满足企业使用的 Enterprise Edition 版，以及提供了实时数据库、网络集成服务、企业资源规划 (ERP) 等组件的 Datacenter Edition 版。这四个不同的版本在功能上都有着很大的差异。

* Windows Server 2003 Web Edition：支持 2GB 内存和 2 路处理器，针对 Web 服务进行了优化，仅能够在 AD 域中用做成员服务器，不能用作 DC (Domain Controller，域控制器)。

* Windows Server 2003 Standard Edition (标准版，对应 Windows 2000 Server)：支持 4GB 内存，4 路处理器，针对中小型企业设计。具备除目录服务 (MMS) 支持、终端服务会话目录、集群服务以外的所有服务功能。

* Windows Server 2003 Enterprise Edition (企业版，对应 Windows 2000 Advanced Server)：支持 64GB 内存和 8 路处理器。针对高端服务的需求设计，具备所有服务功能。

* Windows Server 2003 Datacenter Edition (数据中心版，对应 Windows 2000 Datacenter Server)：支持 512GB 内存和 32 路处理器，符合最高性能的要求，具有极其可靠的稳定性与扩展性。具备除 Internet 连接防火墙、Internet 连接共享以外的所有服务功能。



注意

除了有四个 32 位版本外，Windows Server 2003 中，还增加了对 Intel 安腾 64 位电脑的支持（两个版本），即 Windows Server 2003 Enterprise Server 64-Bit Edition 和 Windows Server 2003 Datacenter Server 64-Bit Edition。

因为是针对网络环境设计的操作系统，所以 Windows Server 2003 的网络功能非常的丰富，说用几本书来介绍也不为过。所以，本书涉及的网

络应用仅是此操作系统的一部分。

5. Windows Vista

Microsoft Windows Vista 是继 Windows XP 之后推出的又一个重要的 Windows 版本，作为一个大幅改变了以往 Windows 使用习惯的操作系统，在 2005 年 7 月 22 日太平洋标准时间早晨 6 点，微软正式公布了这一名字。

未来的几年里，安装及应用 Windows Vista (以下简称 Vista) 将是一种趋势。Vista 为我们带来了一个清晰而透明的世界，帮助我们更容易地进行各种电脑应用。

Windows Vista 共提供了六个版本，每个版本都对应了相应的用户群体。比方说，小型企业、中型企业和大型企业、家庭用户使用的 Vista 就分别有适用的版本和增强版本。

* Home Basic：这是一个入门级版本。它具有容易配置的特点，对于仅仅希望使用电脑上网冲浪、与家人和朋友进行邮件收发、建立和编辑简单文档的用户来说，此版本可以提供一个更安全、更可靠、更容易使用的环境。

* Home Premium：这是一个具有完整功能的增强型版本。它适合于桌面电脑和移动 PC 用户使用，它除了提供 Home Basic 所有的功能外，还提供了 Aero 用户界面、媒体中心功能、DVD 制作等数字媒体功能、Tablet PC 功能，以及 PC To PC 的同步特性。使用此版本的用户，可以享受更加简单和安全的查找、电脑彼此交互的功能，可以使用、组织以及共享照片、视频、电视节目和音乐，可以让管理财务、完成工作、观看电影、收听歌曲、游戏变得更富有乐趣。

* Business：适用于各种规模企业使用的版本。此版本最大的特点就是提供了核心的企业应用特性，如加入域、组策略的支持，以及加密文件系统功能，等等。

* Enterprise：适用于各种规模企业使用的增强型版本，可以满足全球化的、具有高度复杂 IT 架构的组织需求。此版本除了包含 Business 版本中所有的功能外，还包含 BitLocker Drive Encryption、All Worldwide Interface Languages、

第三章 操作系统的选择与安装

Virtual PC Express、Subsystem For UNIX Applications (SUA) 等特性。这个版本可以帮助系统/网络管理员减少部署和管理电脑的成本和复杂度，并可以很好地与企业的信息策略相结合，如可以与合作伙伴、企业随时保持良好的连接。

* Ultimate：对于普通用户或小型企业用户来说，使用 Ultimate 版本非常适合。这个版本有些类似于 Windows XP 的专业版 (Professional)，此版本中包含了跨越所有用户类型的操作系统特性。值得一提的是，它已经具备高级的数据保护功能：Windows BitLocker Drive Encryption。

* Starter：此版本专门供使用较低硬件配置（仅限 32 位）的家庭和入门用户使用，它具有和 Basic 版本相同的用户界面。

从网络环境这个角度来看，部分版本的 Vista 的网络功能还是很强大和丰富的。在本书中，将从组建中小型局域网这个角度谈 Vista 的网络应用，因此使用的版本是 Ultimate。

6. Windows Server 2008

Windows Server 2008 是微软下一代服务器操作系统，主要面向企业用户设计，作为 Windows 2000 (Advanced) Server、Windows Server 2003 的升级版本，还融入了很多 Windows Vista 操作系统的特性。

Windows Server 2008 也有多个版本，即：Windows Server 2008 Standard、Windows Server 2008 Enterprise、Windows Server 2008 Datacenter、Windows Web Server 2008、Windows Server 2008 for Itanium-Based Systems。在本书中，使用的是 Windows Server 2008 Enterprise 这个版本。

3.1.3 Linux 家族

Linux 是目前全球最大的一个开源式操作系统，它是一个可与 Unix 和 Windows 相媲美的操作系统，具有相当完备和强大的网络功能。Linux 最初由芬兰人 Linus Torvalds 开发，其源程序在 Internet 网上进行开源式的公布以后，引起了全世界电脑爱好者的开发热情，许多人下载该源程序

并按自己的意愿完善某一方面的功能，再传到因特网上，Linux 也因此被雕琢成为一个全世界最稳定的、最有发展前景的操作系统。



自由世界的Linux

作为操作系统中的亮点，Linux 究竟魅力何在？Linux 为何能受到人们的广泛喜爱？IBM 这样的国际型大公司为什么也全力支持 Linux？似乎有着无数的答案可以回答这一切，但其中最吸引人的还是以下几点：

* 支持多任务

多任务是现代操作系统最主要的一个特点，作为 Windows 最具吸引力的特性，Linux 同样具备！而且由于 Linux 采取了内存保护模式设计，所以 Linux 可以有效避免因为一个程序的执行失败而使整个系统死机的情况发生。

* 支持多用户

这意味着系统资源可以被不同用户各自拥有及使用，即每个用户对自己的资源（例如文件、目录等）有特定的权限，互不影响，每个用户还具有彼此隔离的主目录。这些特性和 Windows 2000/XP 的多用户管理有着异曲同工之妙！

* 完善的网络功能

由于 Internet 是在 UNIX 领域中建立并繁荣起来的，TCP/IP 最初就是在 UNIX 上测试通过的，所以 UNIX 系统天生支持 Internet。而用户完全可以将 Linux 看成 UNIX 系统在个人计算机上的一个版本，Linux 几乎可以不加修改地运行原本为 UNIX 而编写的应用程序，任何用户都可以很方便地使用 Linux 提供的完善而强大的网络功能，例如个人用户可以免费创建企业级服务器。



* 可靠的系统安全性

Linux 采取了许多安全技术措施，包括对读、写进行权限控制，带保护的子系统，审计跟踪，核心授权等，这为网络多用户环境中的用户提供了必要的安全保障。同时由于采用开放代码设计，可以确保及早发现问题并解决。Linux 发行版本的更新换代速度很快，例如 Red Hat Linux 几乎每 6 个月就有新的版本发布，而当中的补丁更是层出不穷。

* 良好的兼容性

Linux 支持广泛的硬件设备，从 Intel 386 到 Pentium 4 处理器，Linux 支持所有的 x86 平台，这意味着个人 PC 也能够很好的运行。在网络软件支持方面，Linux 支持 TCP/IP、E-mail、X Windows、NFS、NIS、News 及 WWW 等网络服务。

* X Window

Linux 主要的优点之一，X Window 就是 Linux 下独立的桌面环境组件，有 Gnome 和 KDE 两种常见的环境。和 Windows 不同的是，Linux 桌面环境可以看成是在终端上运行的一个应用程序（Client/Server 应用），易于安装和改版，甚至去除，而 Windows 的桌面环境是操作系统内核的一部分，无法分离。

从发展前景上看，Linux 取代 UNIX 和 Windows 还为时过早，但一个稳定性、灵活性和易用性非常好的软件，肯定会得到越来越广泛的应用。

3.2 安装 Windows Server 2003 SP2

初期的 Windows Server 2003 被命名为 Windows .NET Server 2003，其主要原因是系统支持连接 .NET 技术的核心功能。但不久后，微软就正式宣布这个版本的系统被命名为 Windows Server 2003 了。名称虽然又沿袭了 Windows 家族的习惯用法，但从其提供的各种内置服务以及重新设计的内核程序来说已经与 Windows 2000/XP 版有了本质的区别。下面，将讲解 Windows Server 2003 Enterprise Edition SP2 的安装过程。

3.2.1 硬件兼容性

从 Windows 2000 开始，Windows 就对硬件环境有了兼容性限制的做法，这在一定程度上保证了系统安装后的稳定性，是一种值得推荐的做法。

为了让用户能够快速了解自己的硬件系统是否能符合 Windows Server 2003 的要求，微软公司提供了两种方法供读者查询：

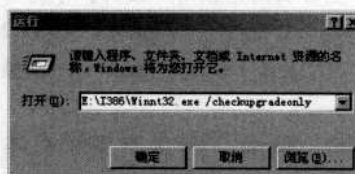
一是访问查询网站。微软特别安排了一个网站，专门介绍 Windows Server 2003 支持的硬件设备，读者们可以通过访问以下网站来获知自己的硬件是否能“过关”：

<http://www.microsoft.com/windows/catalog/server/default.aspx>

二是使用 Windows 升级顾问检测硬件兼容性。在将 Windows Server 2003 安装光盘放入光驱后，依次点击“开始”、“运行”，在弹出的“运行”对话框中输入如下格式的命令：

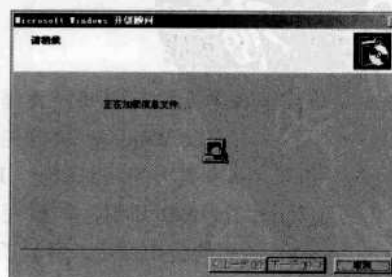
光盘所在盘符：\I386\Winnt32.exe /checkupgradonly

输入命令并回车后，即可运行“Windows 升级顾问”来检测硬件的兼容性是否符合当前需安装系统的硬件要求了。



输入命令

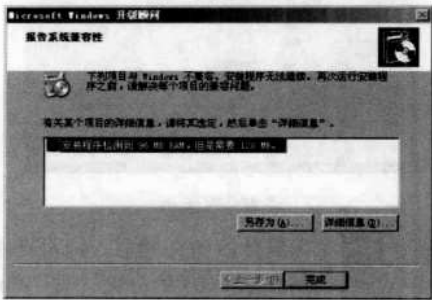
稍后，“Windows 升级顾问”将会被运行，此时请停止系统中其他操作，等待“Windows 升级顾问”加载信息文件的操作完成。



运行升级顾问

第三章 操作系统的选择与安装

接着，“Windows 升级顾问”将会自动对当前硬件进行兼容性检测，并告诉用户问题所在，例如下图中可以看出安装程序检测到当前硬件只有 96MB 内存，如果想解决这个兼容性问题则需要 128MB 内存。



检测结果

瞧，内存不符合兼容性的要求，就是这么既简单又明了的检测出来了，大家都学会了吗？当然，随着 Windows Server 2003 渐渐深入人心，现在的硬件设备大多已经支持 Windows Server 2003 了，不过最好还是不要主观地认为硬件已经位于 HCL 列表里，最好使用带有“Designed for Windows”标签的硬件设备。

最后再来看看微软对 Windows Server 2003 安装时最低的硬件的需求，如表 3-1 所示。

表3-1

处理器	550 MHz Pentium/Celeron 系列、AMD K6/Athlon/Duron 系列或兼容的中央处理器
内存	最小 128MB 内存，推荐 256 MB 内存以上
磁盘空间	2 GB 硬盘
光驱	对于光驱安装，需要 CD-ROM 或 DVD 驱动器支持
软驱	如果不能访问光驱，可以采用软盘+光盘映像文件的方法

如果用户系统不能满足上表要求，那么 Windows Server 2003 很可能是不会“屈尊下嫁”到你的计算机中的。

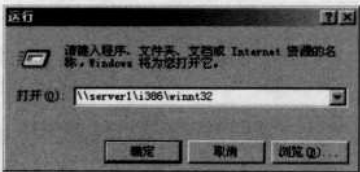
3.2.2 安装实战

Windows Server 2003 安装可以使用多种方式，下面来了解一下最常见的三种安装方式：

> 从光盘安装：适用于从现有系统升级、全新安装；适用于裸机安装；

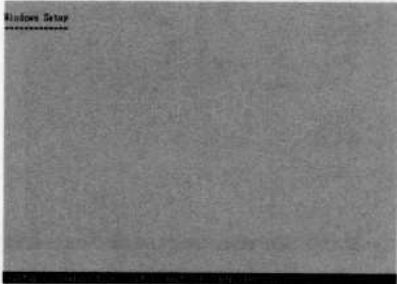
> 从软盘安装：适用于 DOS 安装；适用于裸机安装；

> 从网络安装：适用于局域网安装。其方法大致为，将 Windows Server 2003 光盘目录中的 I386 目录复制到局域网中的某台计算机上，并设为共享目录。此时网络上其他计算机即可执行此目录中的“Winnt32”文件进行安装。



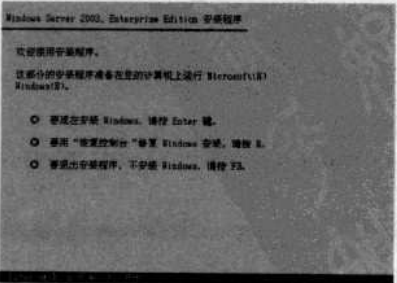
网络安装

STEP 1 在启动计算机并在将 Windows Server 2003 的安装光盘放入光驱后，安装程序将首先开始从光盘向硬盘上复制一些安装时需要的临时文件。



加载硬件基本信息

STEP 2 文件复制完毕后，将自动进入文本模式（蓝底白字）安装界面时，安装程序将会询问是否进行 Windows Server 2003 的安装。

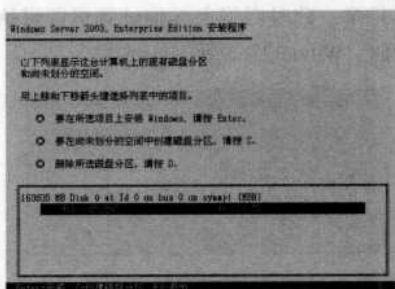


选择菜单

STEP 3 在按下“Enter”键后，稍后的安装

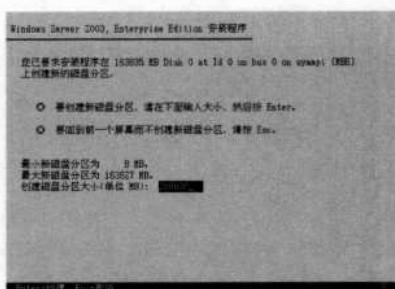


基本上与安装 Windows XP 相同——在弹出的提示阅读和接受最终用户许可协议界面中按 F8 键接受协议要求后继续。在出现提示选择哪个分区安装 Windows Server 2003 时，因为当前硬盘是还未进行分区的硬盘，所以应按“C”键继续。



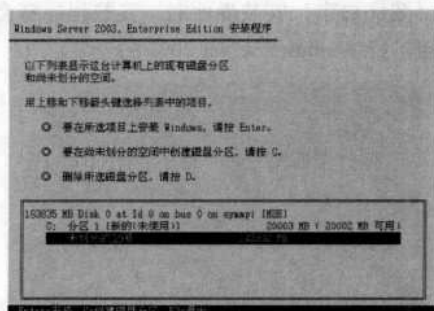
分区状态

STEP 4 下一步中输入第一个分区的容量大小后按“Enter”键即可创建该分区。



创建第一个分区

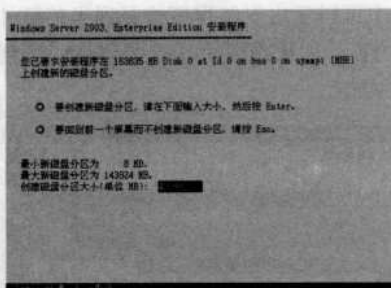
STEP 5 在返回到上一步后，选择剩余的未进行分区空间并按“C”键进入创建分区界面。



选择剩余空间

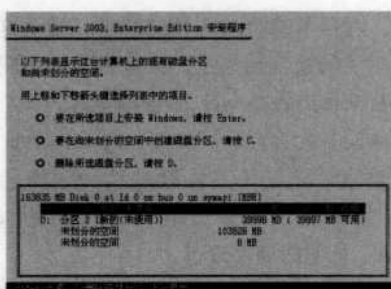
STEP 6 在进入界面中根据需要设置好第二个分区容量并按“Enter”键即可完成分区的创建。

重复这个操作即可完成将一块硬盘完成 N 个分区的操作。



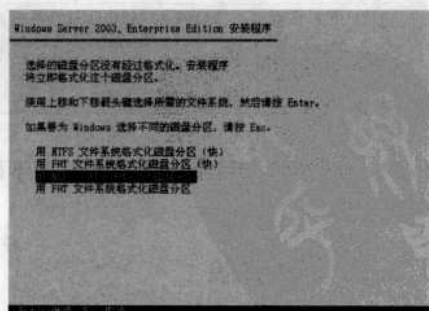
设置分区大小

STEP 7 在完成分区的创建后，即可选中准备安装 Windows Server 2003 的分区并按“Enter”键继续了。



选择安装到的分区

STEP 8 下一步中安装程序将告诉我们选择的分区没有格式化，并要求我们选择一种最适合当前操作系统使用的格式分区格式化操作，建议选择“用 NTFS 文件系统格式化磁盘分区”项继续。



选择文件系统

STEP 9 稍后安装程序将开始对当前分区按指定格式进行格式化操作。

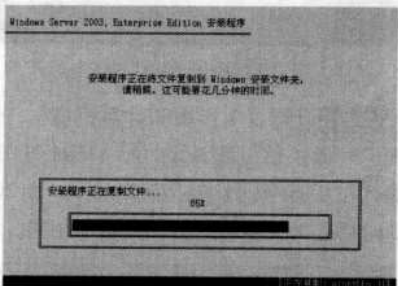
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三章 操作系统的选择与安装



格式化进度

STEP10 格式化完毕后，安装向导将开始磁盘检查并进行文件复制操作，文件复制完毕后重新启动计算机。



复制进度

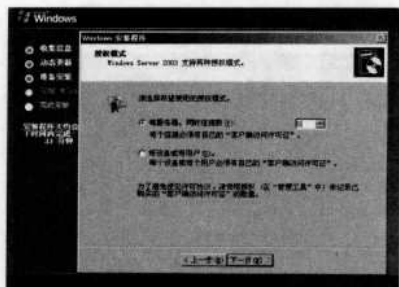
STEP11 稍后将可以看见 Windows Server 2003 的首次运行画面了，如图所示将会一闪而过。



启动界面

STEP12 接着安装进程将进入图形界面安装部分，并自动启动安装向导。

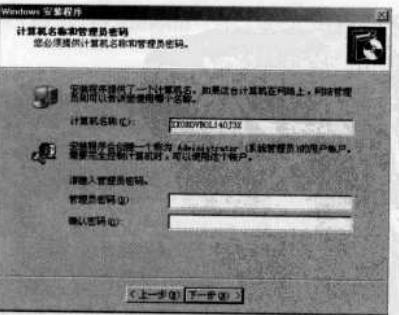
STEP13 接下来将会出现“区域设置”和“自定义软件”、“软件密钥”，在根据需要输入信息后，点击“下一步”按钮继续。在进入授权模式选择这一步时，我们可以发现 Windows Server 2003 服务器支持两种授权模式：每客户和每服务器。



设置授权模式

如果选择了每客户模式，每台访问 Windows Server 2003 服务器的计算机都要求有自己的客户端访问许可证 (CAL)。使用一个访问许可证，一个特定的客户端计算机可以连接到任意数量的 Windows Server 2003 服务器上。对于拥有超过一台 Windows Server 2003 服务器的公司来说，这是最常用的授权方法。相反，每服务器授权意味着每一个与服务器的并发连接都需要一个单独的访问许可证。这意味着在任何时候，这台 Windows Server 2003 服务器都可以支持固定数量的连接。例如，如果选择了每服务器客户端授权模式和五个并发连接，此 Windows Server 2003 服务器可以同时被五台计算机（客户端）所连接。这些计算机将不需要任何其他许可证。只有一台 Windows Server 2003 服务器的中小企业通常选择每服务器授权模式。为了服务器的可扩展性，我们这里选择每服务器授权模式。然后点击“下一步”按钮。

STEP14 在进行到输入管理员密码一步时，则一定要输入规范有靠的安全密码。

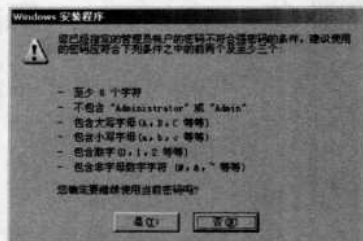


设置密码

那么什么是安全的密码呢？如果你输入密码不符合要求，那么安装程序将马上会弹出提示框，



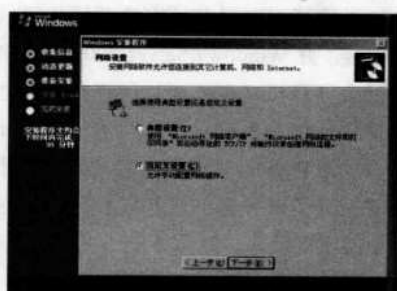
从中可以看到推荐的密码组合形式。



密码强度提示

STEP15 在下面的“时间和日期”设置时可以直接点击“下一步”继续，在进入“网络设置”界面时既可以选择默认值，直接点击“下一步”按钮继续，也可以进行手工设置。以手工设置为例，方法如下：

其实这里的设置就是进行网卡属性的设置，如果用户有安装 Windows Server 的基础且对自己的网络比较熟悉，建议选择“自定义设置”，由用户自己动手设置网卡的 IP 地址、子网掩码、网关和 DNS 服务器地址。点击“下一步”按钮继续。



设置网络

STEP16 接着选择“Internet 协议 (TCP/IP)”，然后点击“属性”按钮。



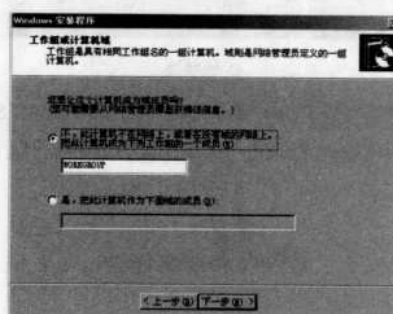
设置网络协议

STEP17 在随即弹出的对话框中输入 IP 地址、子网掩码、网关和 DNS 服务器等信息，如果网内还没有服务器提供 DNS 服务，那也没有关系，这里可以先空着，以后再修改。接着点击“确定”按钮退出设置继续安装。



设置IP内容

STEP18 设置“工作组和计算机名”一步时，请注意了，如果想组建 Windows server 2003 局域网，那么在所有电脑安装 Windows server 2003 到这一步时都应将工作组的名称设置为相同。



设置工作组



注意

如果该服务器是域中的一台，这里应该将该服务器加入域。

STEP19 稍后安装程序将开始各种组件的配置和安装，安装完毕并重启后虚拟机后，将出现 Windows Server 2003 的登录提示框。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三章 操作系统的选择与安装



登录对话框

STEP 20 按“Ctrl+Alt+Delete”组合键后，将会出现登录对话框。



输入登录账户及密码

STEP 21 在输入系统安装时设置的管理员密码后，按下回车键即可进入 Windows Server 2003 的桌面了。至此，Windows Server 2003 的安装就彻底结束啦！

3.3 安装Vista Ultimate

Vista 是一个博大精深的操作系统，它是数千名顶级程序员不懈努力的心血结晶，是在收到数十万测试用户的意见反馈后，不断“去糙存精”的科学成果。在本例中，将讲解全新安装 Vista Home Premium 的方法。

3.3.1 安装环境

在计算机中安装 Vista，可以使用很多种方法，即：

- > 升级安装：推荐所有用户都来了解这种安装方式，但不推荐使用这项安装方式。
- > 全新安装：如果常用的应用软件和主要硬件的驱动，都能稳定在 Vista 中运行时，则推荐用户安装使用。
- > 双系统安装：推荐准备对 Vista 尝鲜的新手

使用。

- > 硬盘安装 Vista：没有 DVD 光驱 / 刻录机但却想安装 Vista 的用户使用。

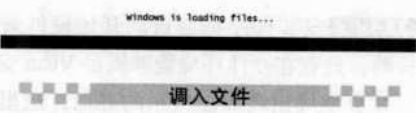
本书用于测试安装此版本的硬件环境为：

- > 硬盘：200GB 的全新、未分区硬盘
- > 内存：512MB
- > 光驱：DVD-ROM

3.3.2 安装实战

由于 Vista 不同版本的安装过程都是一样的，所以，其他版本的 Vista 安装也可以参考下面的方法执行。

STEP 1 把 Vista 安装光盘放入光驱并启动，在看到如图所示的界面时，表示正在使用 Vista 安装光盘启动且正在调入文件。



STEP 2 在出现如图所示的界面时，需要选择要安装的语言类型、时间和货币格式，以及键盘和输入方式。这里，通常都是选择默认设置并直接单击“下一步”按钮。



STEP 3 在出现如图所示的界面时，直接单击“现在安装”按钮继续。



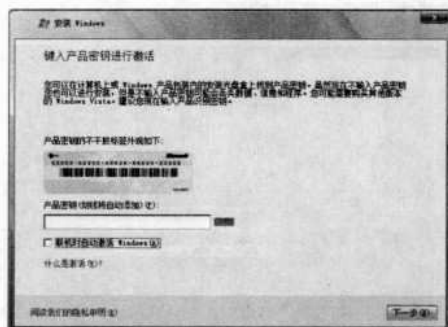
单击“现在安装”按钮



注意

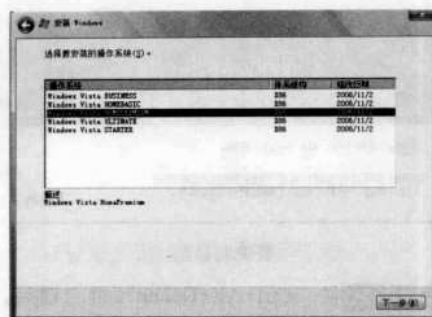
如果希望对即将安装的 Vista 进行初步了解，可以单击左下角的“安装 Windows 须知”按钮，在打开的帮助窗口中看到相关的知识。

STEP 4 安装程序将会自动开始硬件兼容环境的检测，只有在硬件环境能够满足 Vista 安装需求时，才会继续出现如图所示的界面。这里需要输入 Vista 产品包装中附带的 25 位产品序列号，由于中间的分隔符会自动输入，所以只需输入字母和数字即可。



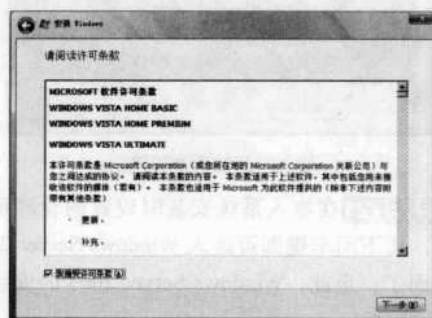
输入序列号

STEP 5 清空“联机时自动激活 Windows”项并单击“下一步”按钮后，将会出现“选择要安装的操作系统”界面。此时，需要在列表中选择“Windows Vista Home Premium”项。



选择Vista版本

STEP 6 在出现许可条款界面时，勾选“我接受许可条款”项单选框并单击“下一步”按钮继续。



许可协议

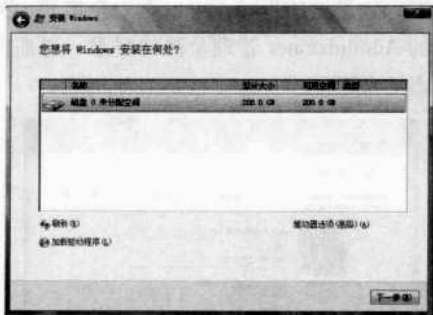
STEP 7 在出现安装类型选择界面时，可以选择安装类型为升级或自定义（高级）。其中，升级安装的选项要满足多个条件方可激活可选状态（请见本书升级安装一章中的内容）。此外，如果使用安装光盘启动并执行 Vista 的安装，则这里的升级选项同样也是不可用的，所以此时只能选择“自定义（高级）”项继续。



选择自定义安装

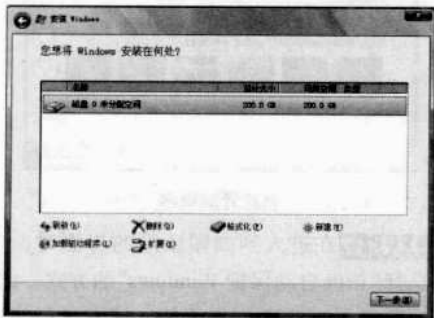
第三章 操作系统的选择与安装

STEP 8 由于是在全新电脑中安装 Vista，硬盘还没有进行分区和格式化操作，所以在出现如图所示的界面时，可以看到可用空间为当前硬盘的全部空间。



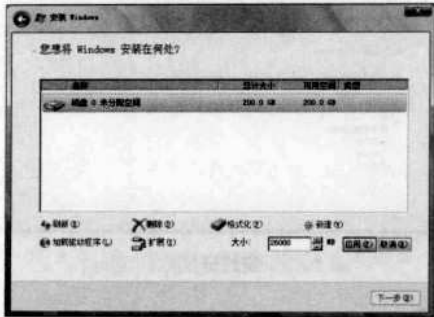
分区状态

STEP 9 由于硬盘没有进行分区和格式化操作，就不能进行 Vista 的安装。所以，此时需要先对硬盘执行分区和格式化操作。执行这个操作可以有两种方式，一是选中硬盘并直接单击“下一步”按钮，这样将一块硬盘可以直接划成一个分区，并在这个分区上执行安装操作。这种方式对于容量动辄数百 GB 的硬盘来说很不现实。二是对当前硬盘进行多个分区的划分后，再在 C 盘分区中执行格式化操作以及进行 Vista 的安装。如果要对硬盘进行分区，则需单击“驱动器选项（高级）”项切换到如图所示的界面，此时即可对硬盘进行新建、删除、格式化、扩展分区等操作。



创建分区

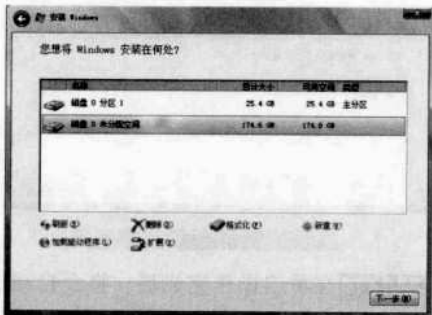
STEP 10 在单击“新建”按钮后，将会切换到如图所示的界面。



设置分区大小

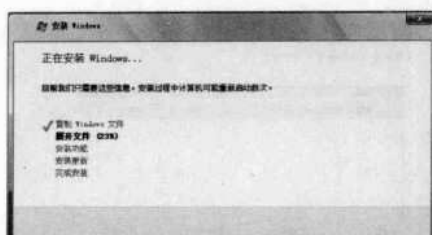
这里需要输入创建的第一个分区的大小数字，由于 Vista 只能被安装在 NTFS 格式分区下，并且分区剩余空间必须大于 8GB。所以，这里建议输入大于 15GB 的数字，如 26000（单位为 MB，即 26GB 左右）。

STEP 11 在单击“应用”按钮切换到的界面中，选中上方列表中的剩余空间并单击“新建”按钮。接着，在随即出现的“大小”栏中输入第二个要创建的分区大小。重复这个操作，可以完成所有分区的创建。



新建分区

STEP 12 在完成分区的创建并在上方的列表选中准备安装 Vista 的分区后，单击“下一步”按钮继续。在出现如图所示的界面时，安装程序将会自动对选中的分区执行格式化操作，并将安装光盘中的某些文件复制到硬盘中并展开（由于安装光盘中的文件是压缩的，且光盘中无法执行解压操作，所以要将其复制到硬盘并解压。）。



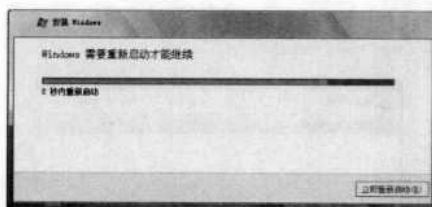
安装进度



注意

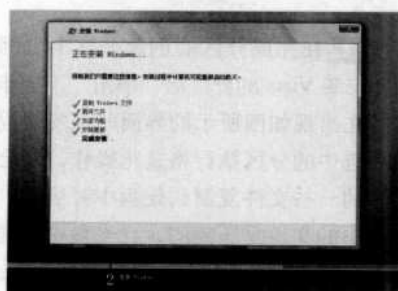
如果在安装时出现“Setup was unable to locate a locally attached hard drive suitable for holding temporary Setup files.”提示，只需将安装 Vista 的分区大小设置为具有 10GB 以上的可用空间即可！其中，分区中有 2GB 的左右剩余空间将作安装文件的临时目录使用。出现该错误的原因，就是无法创建临时文件目录！

STEP13在完成文件的复制及解压操作后，安装程序将会自动执行一次重启操作。



启动进度

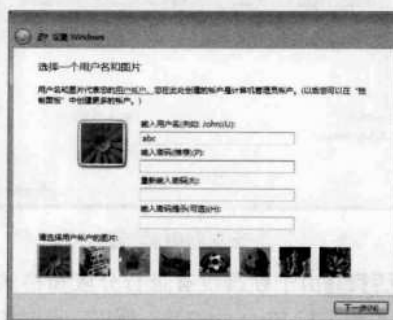
STEP14在重启操作完成后，将会自动进入如图所示的界面，这里将继续前面的安装进度。



继续安装

STEP15当再次重启并出现如图所示的界面

时，这里可以创建一个管理员账户以及设置对应的密码（可以不设置密码）和挑选喜欢的头像。这样，默认的 Administrator 管理员账户会被隐藏起来，如果这里创建的账户在今后的操作中因种种原因导致无法使用时，可以在安全模式中使用默认的 Administrator 管理员账户登录，进而实现账户修复或建新。



新建账户

STEP16在单击“下一步”按钮进入如图所示的界面时，这里需要为当前电脑输入一个名称，并可以在下方的列表中单击选择一个桌面背景图片。操作将会立即被执行，因为在设置界面的下方会产生相应的变化。



创建计算机名

STEP17在进入如图所示的界面时，这里需要选择“帮助自动保护 Windows”的方式。此时，推荐选择第一项全面保护系统，或者选择第三项在今后熟悉此功能后再设置它。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三章 操作系统的选择与安装



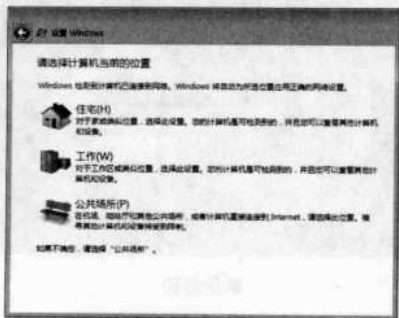
设置安全状态

STEP18在出现“复查时间和日期设置”界面时，如果当前电脑中的时间与日期有偏差，可以在这里调整它。否则，直接单击“下一步”按钮继续。



设置时间

STEP19在出现如图所示的界面时，需要为电脑选择一个所在的局域网络类型，这里选择“住宅”就可以了。



选择网络环境

住宅、工作和公共场所三个网络位置中，如果选择前两者，则意味着允许用户查看网络中的

其他电脑和设备，并允许其他网络用户查看用户的电脑。如果选择的是“公共场所”，则意味着用户的电脑对周围的电脑处于不可见状态（即 Vista 中的“网络发现”功能会被禁用），并且帮助保护电脑免受来自 Internet 的任何恶意软件攻击。



注意

如果网络上只有一台电脑并且无需共享当前电脑中的文件、打印机等资源，则最安全的选择是“公共场所”。

STEP20出现如图所示的界面时，表示 Vista 在使用前的安装与设置操作都已结束，单击右下角的“开始”按钮进入 Vista 的桌面环境。



安装结束

STEP21在进入桌面环境之前，Vista 会自动执行一项重要的任务，这就是检测系统的硬件性能。Vista 会根据检测的结果自动对系统进行调整与优化，这个过程一般需要数分钟。



硬件设备检测



注意

在 Vista 中，硬件共被分为 5 级。对于不同等级的硬件配置，Vista 将会自动进入相应的功能缩减模式，也就是说部分功能将不能自动或被禁止使用。

STEP22 稍后，如果在前面设置了账户密码，则会出现如图所示的登录界面，在这里需要输入密码后再按下 Enter 键。



STEP23 如果没有设置密码，则会直接进入桌面环境。在自动出现的“欢迎中心”窗格中可以看到 Windows Vista Home Premium 的版本标识。



这样，Windows Vista Home Premium 的安装就顺利完成了。

3.4 安装 Windows Server 2008

本例中，将在全新计算机中使用光盘引导的方法安装 Windows Server 2008，简体中文版的安装过程非常容易。由于所有的版本都是集合在一张光盘里的，所以，安装其他版本的 Windows

Server 2008 也可以参考本书的方法执行。

3.4.1 准备工作

要安装 Windows Server 2008，需要在硬件方面至少满足如表 3-2 所示的需求：

表3-2

硬件	具体标准
CPU	1GHz，建议2GHz以上
内存	1GB，推荐4GB
硬盘空间	最小8GB，推荐40GB以上
光盘驱动器	DVD-ROM
显示器	Super VGA (800 x 600) 或者更高级的显示器

- Windows Server 2008 支持多种安装方式，如：
- > 用安装光盘引导启动安装；
 - > 从现有操作系统上全新安装；
 - > 从现有操作系统上升级安装；
- 由于 Windows Server 2008 安装光盘需要使用 DVD 光盘进行存储，所以，安装的过程中需要准备一部 DVD 光驱或 DVD 刻录机。

3.4.2 安装实战

因为 Windows Server 2008 的安装和 Vista 的安装差不多，整个过程比较简单。所以，在下面的内容中，将对安装步骤做适当精简：

STEP1 将 Windows Server 2008 安装光盘放入 DVD 光驱并启动计算机，在加载 boot.wim 文件并启动 WINPE 后，将会出现如图所示的界面。



STEP2 在出现如图所示的界面时，单击“现在安装”按钮继续。

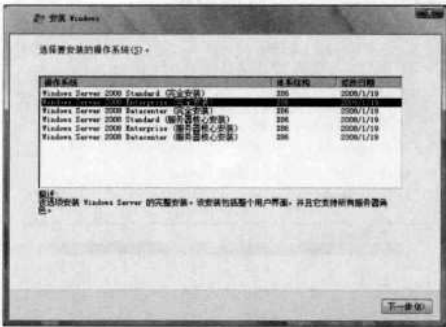
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三章 操作系统的选择与安装



单击“现在安装”

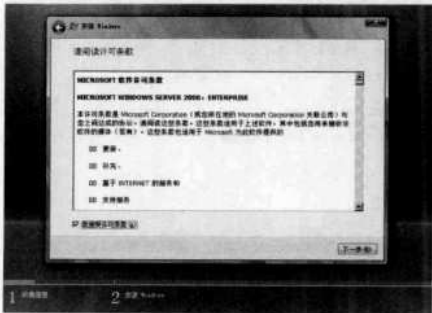
STEP 3 在出现如图所示的版本列表时，选择 Windows Server 2008 Enterprise（完全安装）版继续。



选择要安装的版本

STEP 4 在出现输入安装序列号界面时，输入所选 Windows Server 2008 版本的安装序列号。

STEP 5 在出现如图所示的许可条款界面时，勾选“我接受许可条款”项继续。



许可协议

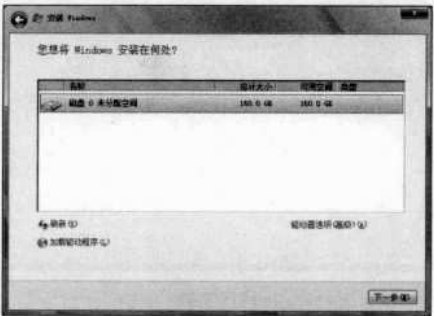
STEP 6 在出现如图所示的界面时，因为是在全新的计算机中安装此系统，所以“升级”项会自动禁用。因此，只能单击“自定义（高级）”项继续。

项继续。



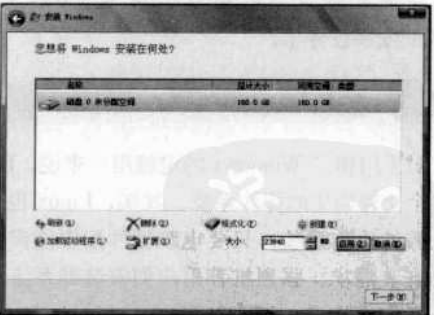
选择自定义安装

STEP 7 在出现如图所示的界面时，选中列表中的项目并单击“驱动器选项（高级）”按钮。



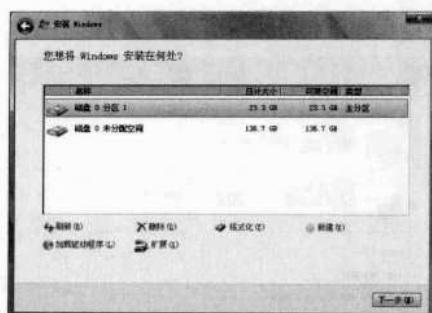
分区状态

STEP 8 在下方出现的文本框中输入第一个分区的大小数字后，单击“应用”按钮。



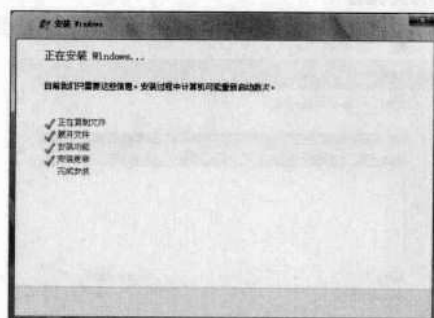
设置第一个分区大小

STEP 9 在完成分区的创建并返回到如图所示的界面后，选中创建的分区并单击“下一步”按钮继续。



选择第一个分区

STEP 10 接着将会执行文件复制、解压等一系列的安装操作。



执行安装

STEP 11 连续两次重启并完成一系列的自动设置后，就可以看到登录界面，在这里可以使用空密码或创建一个新密码进行登录。

在完成登录后就可以结束 Windows Server 2008 的安装任务了。

3.5 安装Linux

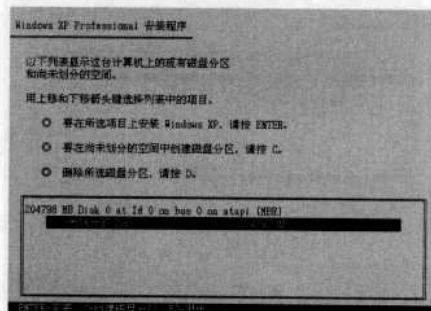
对于用惯了 Windows 的电脑用户来说，Linux 是一个比较陌生的操作系统。其实，Linux 也是一个很棒的操作系统，只要电脑硬件配置能满足系统的安装需求，强烈推荐用户们安装此系统来感受一下它的风采。在网络环境中，Linux 是一个服务器系统，它一般不会安装到客户计算机中。下面，将讲解安装 Windows XP 和 Fedora Core 8.0（以下简称 FC）双系统的方法。

3.5.1 准备工作

Linux 有好多版本，如 Debian、SuSE、Archlinux、Mandrakelinux 以及 Slackware 等。FC 是一个独立的操作系统，只是 Linux 的一个版本。因为 Linux 是开放源代码的操作系统，所以技术精通的用户完全可以做出自己的 Linux 发行版！

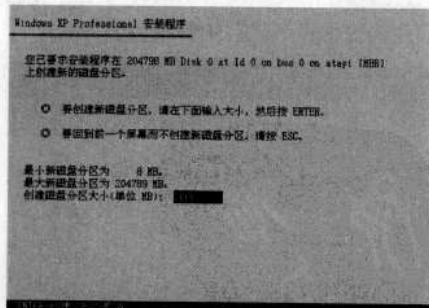
在准备工作中，需要了解 Windows XP 的安装过程中的分区设置操作最为重要，这是因为 Linux 与 Windows XP 使用的空间类型是不一样的，所以在分区时需要分别预留出供 Windows XP 和 Linux 使用的空间。为此，需要执行如下操作：

STEP 1 当出现如图所示的界面时，需要按下 C 键开始第一个分区的创建。



分区状态

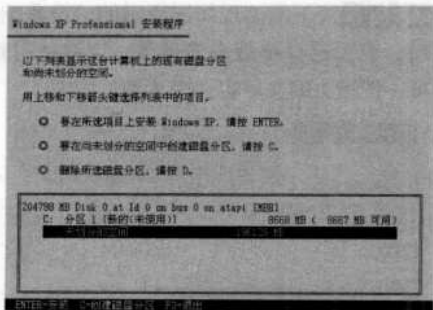
STEP 2 在出现如图所示界面时，首先划分出第一个分区，用于安装 Windows XP 时使用。



设置第一个分区大小

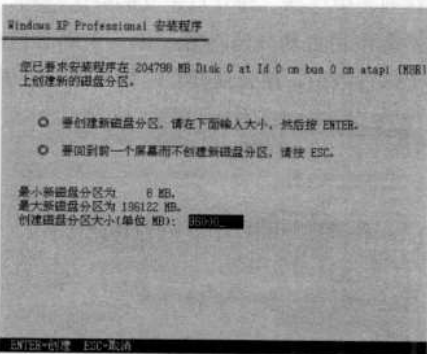
STEP 3 返回到如图所示界面时，选中“未划分的空间”并再次按下 C 键。

第三章 操作系统的选择与安装



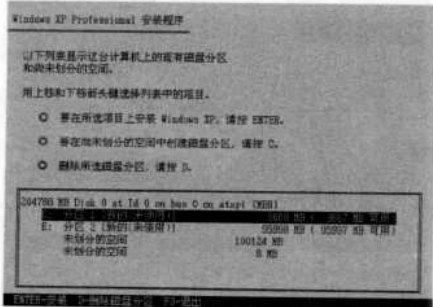
选择剩余空间

STEP 4 在如图所示的界面中，输入一个表示即将创建的分区大小的数字，为 Windows XP 预留一些存储其它数据的空间。只要空间足够，我们可以重复这个创建分区的过程，为 Windows XP 保留足够多的分区，以供其使用。



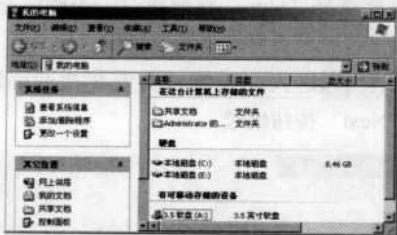
设置第二个分区大小

STEP 5 返回到如图所示的界面后，不要理会“未划分的空间”，因为这些空间是预留给 Linux 使用的。因此，现在需要选中 C 盘分区，并按下 Enter 键在 C 盘分区上安装 Windows XP。



选择要安装系统的分区

STEP 6 接着，依次进行 C 盘分区的格式化、文件的复制等操作，将 Windows XP 安装完成。在安装 Windows XP 完毕后，打开如图所示的“我的电脑”窗口时，可以看到已经格式化并使用的 C 盘和未进行格式化的 D 盘，但是不能看到“未划分空间”的那部分空间。



看不到未划分空间

这样，就完成了 Windows XP 的安装，并在空间上做好了安装 Linux 的准备工作。下面，就可以开始 Linux 的安装了！

3.5.2 Linux 安装实战

在“<http://mirror.linux.duke.edu>”中完成 FC 的 DVD 格式的 ISO 映像安装文件下载（名称为 Fedora-8-i386-DVD.iso，大小为 3.18GB）后，使用 Nero 的刻录映像文件功能将其刻录成 DVD 安装光盘。接下来，需要执行如下的安装操作：

STEP 1 首先，需要将 BIOS 中第一启动设备设置为光驱。接着，在将 FC 光盘放入光驱后，将出现如图所示的欢迎屏幕。



欢迎屏幕

这里如果直接按下“Enter”键，将使用默认的图形界面安装；如果想以文本模式的安装，则需要选择第二项“Install or upgrade existing”



system(text mode)”;如果想修复已经安装好的系统，则需要选择第三项“Rescue installed system”；如果要从硬盘启动，就选择第四项“Boot from local drive”（在本例中选择此项将会启动已经安装好的 Windows XP）。

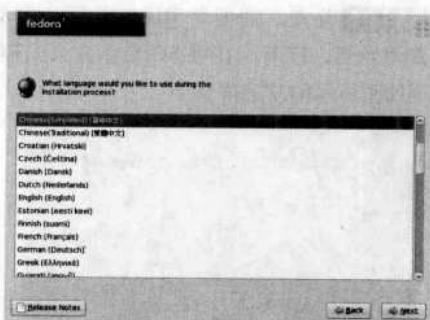
STEP 2 选择第一项并回车后，将会出现界面，需要选择“Skip”直接跳过。否则就会等长时间进行光盘完整性的检查操作。

STEP 3 进入如图所示的安装欢迎屏幕时，单击“Next”按钮继续。



欢迎屏幕

STEP 4 进入如图所示的“Language Selection”页面后，可以在窗口右侧选择安装过程所使用的语言，此处自然是选择“中文简体”。随即，安装程序的界面将换成中文界面。

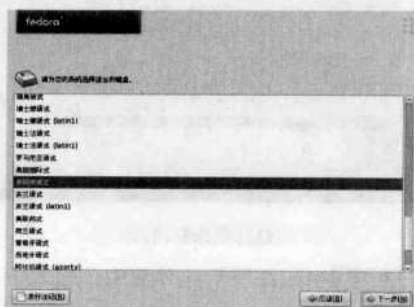


选择中文简体



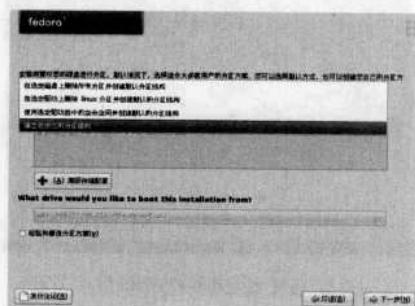
如果内存太小，则 Linux 安装程序会给出“因内存太小无法启动图形界面”的提示，并强制使用文本模式。

STEP 5 接下来出现如图所示的“键盘配置”界面时，需要选择键盘布局类型，这里使用默认值即可，按钮上的文字也会变成简体中文。



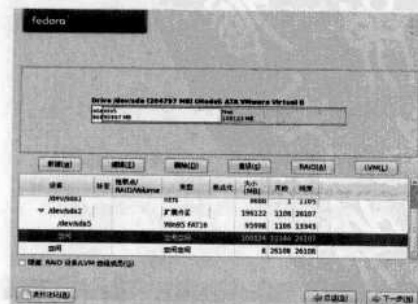
键盘配置

STEP 6 在如图所示的界面出现时，因为电脑中还有其他的操作系统，即 Windows XP，所以必须在列表中选择“建立自定义的分区结构”项。这里不能使用自动分区功能，因为自动分区功能将会把磁盘清空，这会使其他的操作系统丢失。



分区设置

STEP 7 在进入如图所示的界面后，单击选中未进行分区操作的自由空间（就是分区魔术师划出来的那部分空间）并单击“新建”按钮。



新建分区

第三章 操作系统的选择与安装

STEP 8 对于初学者来说，接下来至少需要创建三个分区，即“/”分区、“/boot”分区和“Swap”分区。出现如图所示的窗口后，首先创建引导分区（即“/boot”分区），将挂载点设置为“/boot”，容量可以是 100MB，文件系统是 ext3。

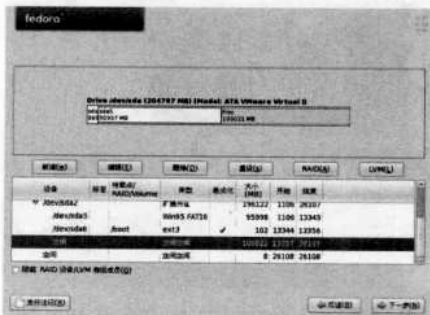


创建分区

注意

何谓挂载点？在 Linux 环境下是没有 Windows 的 C、D 盘符概念的，每一个 Linux 分区必须挂载到 Linux 目录树上才可以使用。这里有一个特殊的分区，就是根目录“/”，这个目录是必须要有的，它是 Linux 目录树的根。

STEP 9 单击“确定”按钮返回到如图所示的界面，选中剩下空闲空间，并单击“新建”按钮。



新建分区

注意

Linux 中每个分区是如何命名的呢？原来，系

统的第一块 IDE 接口硬盘的第 1 分区被称为“/Dev/Hda1”；第二个分区被称为“/Dev/Hda2”，其下分区名称以此类推即可。

STEP 10 接着出现的如图所示界面中，需要创建一个根分区。在弹出的“添加分区”对话框上，选择挂载点为“/”，选择文件系统类型为 ext3，理论上可以将剩余的容量全部分配给根分区，但实际上必须留出一点空间，否则系统会报错。并且，接着要创建的交换分区也需要一定的空间。



设置文件系统类型

STEP 11 单击“确定”按钮返回到上一步后，选中剩下的空闲空间并再次单击“新建”按钮。

STEP 12 在出现的如图所示界面中，需要创建一个交换分区（即所谓的虚拟内存，“Virtual Memory”）。交换分区是一个特殊的分区，用来暂时存放当前不运行的程序和数据，类似于 Windows XP 里的页面文件。它没有挂载点的概念，因此此处需要在“文件类型”中选择 swap 项。它的大小通常要根据物理内存的大小来设置，例如内存容量是 512MB，则交换分区容量可以设为 1024MB。



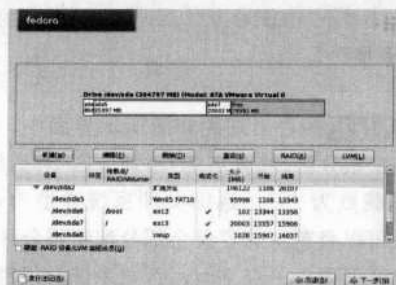
设置分区大小

STEP 13 返回到如图所示的界面后，可以看

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

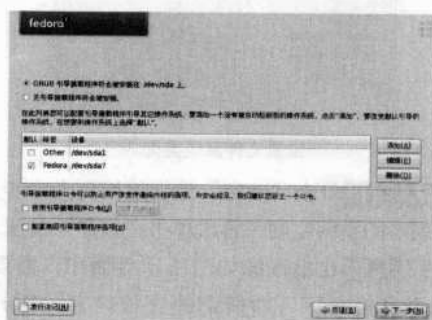


到新创建的三个分区。



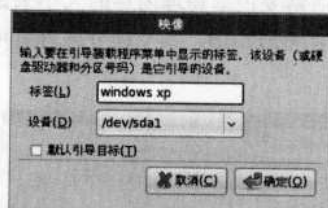
分区状态

STEP14在完成分区的创建后，在接着的如图所示界面中。需要设定多操作系统状态下，默认启动的系统是什么。如果我们希望默认启动 Windows XP，那么就单击选中“Other”项。



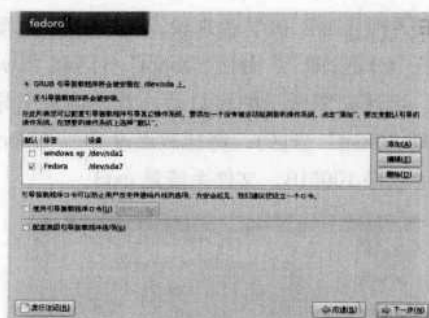
设置默认启动的系统

STEP15不管是否选中 Other 项，都建议单击其右侧的“编辑”按钮，在弹出的对话框中，将标签名由“Other”改为“Windows XP”。



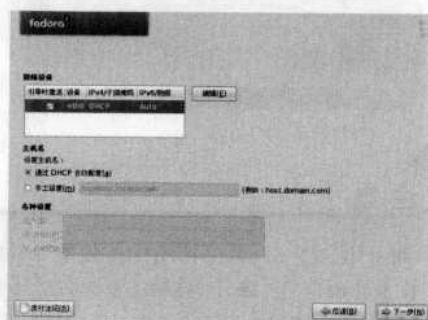
更改名称

STEP16在单击“确定”按钮返回到如图所



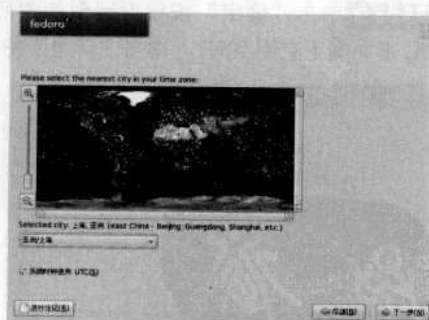
启动名称

STEP17在进入如图所示的界面时，对于非局域网的用户，只需选择默认状态即可。



设置网络

STEP18在如图所示的“请点击地图选择区域”界面中，需要在列表中选择“亚洲/上海”项。



设置区域

STEP19在如图所示的界面中要设置一个 ROOT 账户的密码，这个账户是 Linux 系统中权限最高的账户。它的密码万万不可以丢失，所有重要的系统设置操作都需要使用这个账户。

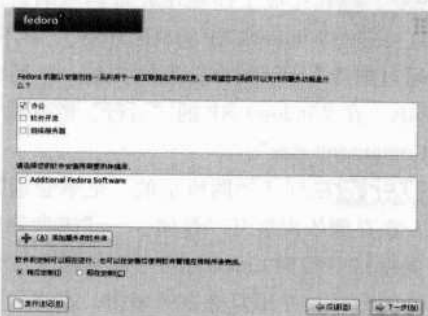
第三章 操作系统的选择与安装

Chapter



设置密码

STEP20在如图所示的界面中，安装向导会询问我们要安装的 Linux 用途。对于刚接触 Linux 的用户来说，选择默认状态即可。



设置安装系统用途

STEP21在出现如图所示的界面时，单击“下一步”按钮开始 FC 的正式安装。



开始安装

STEP22接着，将会进行格式化、将光盘中的安装文件复制到硬盘等操作。



安装进度

STEP23在准备操作完毕后，将会开始安装 FC 的安装。在安装过程中，如果是使用 CD 安装光盘，则需要根据提示不断更改下一张安装光盘。因为使用 DVD 安装光盘，所以这个更换光盘的操作就可以省却了。



更换光盘

STEP24很快如图所示的提示安装完成界面就会出现，此时，需要单击“重新引导”按钮。

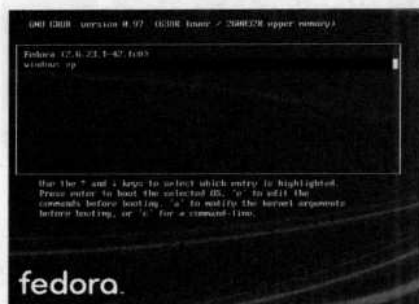


单击“重新引导”按钮

STEP25重启后会看到启动界面。根据提示，此时可以按下任意键进入 Windows XP 和 Linux 双系统菜单，否则将在数秒后自动启动默认的操作系统。



STEP 26 如果按下任意键，则会进入如图所示的双系统菜单界面。在这里可以选择 Windows XP 或 FC 进行登录。



菜单选择界面

这样，Windows XP 与 Linux 双系统的创建就成功结束了。

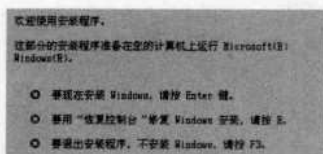


在 <http://support.microsoft.com/kb/919529/zh-cn> 中，可以了解到双系统时如何对启动配置进行管理。

3.5.3 Windows XP中卸载Linux

如何在 Windows XP/Linux 双系统环境中卸载 Linux？这个看起来似乎很头疼的问题，其实操作起来却是非常的容易。在本例中，就将与大家说说卸载的方法。

STEP 1 使用 Windows XP 安装光盘启动电脑，在出现如图所示的界面时，按下键盘上 R 键继续。



STEP 2 在如图所示的界面中，依次执行如下操作：

> 根据提示输入数字 1，选择进入 Windows XP 操作系统；输入管理员密码，登录系统；

> 在“C:\WINDOWS>”命令行中输入命令“Fixmbr”并按下 Enter 键；

❖ 62 ❖

> 在弹出的“确实要写入一个新的主启动记录 (MBR) 吗？”提示右侧，输入字母 Y 确认写入一个新的主启动记录 (MBR)。

```
1: C:\WINDOWS
要登录到哪个 Windows 安装
(要取消，请按 Enter 并 1)
请输入管理员密码:
C:\WINDOWS>fixmbr

** 注意 **
如果继续，FIXMBR 可能会损坏坏的分卷表。
这会造成当前磁盘的所有分区不可访问。
如果访问驱动器没有问题，则不要继续。
确实要写入一个新的主启动记录 (MBR) 吗? y
正在将新的主启动记录写入物理驱动器
\Device\Harddisk0\Partition0 上。
已成功写入新的主启动记录。
```

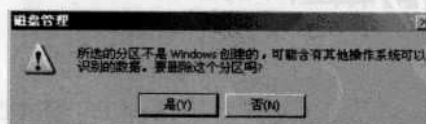
C:\WINDOWS>

STEP 3 在完成上述操作并重启电脑后，就可以直接进入 Windows XP 的桌面环境了。接下来，需要通过删除 Linux 所在分区的方法，来彻底卸载 Linux。在 Windows XP 的“运行”栏中输入命令“Compmgmt.msc”。

STEP 4 在打开如图所示的“电脑管理”窗口中，在左侧依次展开“存储”→“磁盘管理”，在右侧窗格中找到 Linux 分区（即标注为“未知分区”的分区）并用鼠标右键单击，在弹出菜单上单击“删除逻辑驱动器”命令，即可删除该分区。



STEP 5 在接着弹出的如图所示对话框中，单击“是”按钮继续。



STEP 6 重复这个删除未知分区操作，直至把 Linux 的分区全部删除完毕为止。这样，就可以在 Windows XP/Linux 双系统的环境中，彻底卸载掉 Linux 了。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

组网实战篇

第四章 组建家庭局域网

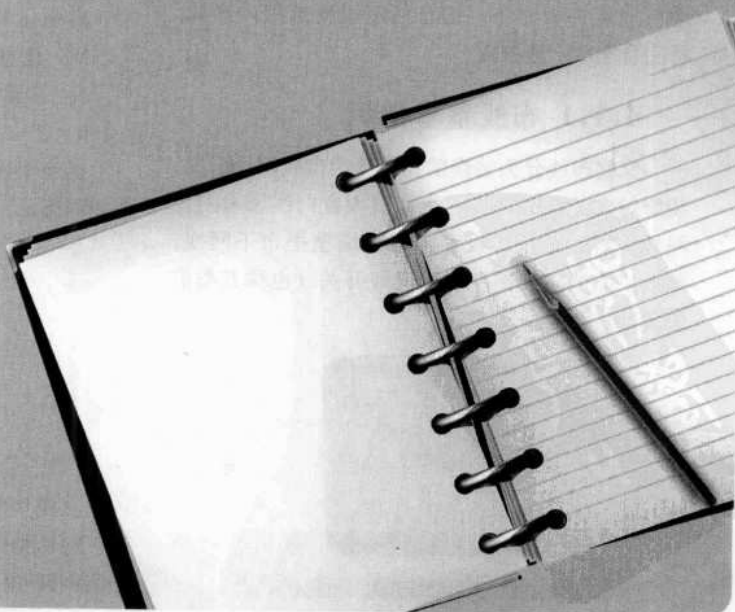
第五章 组建中小型企业网络

第六章 组建校园网

第七章 组建无线局域网

第八章 政府办公楼网络组建

第九章 网吧局域网组建实战



第四章 组建家庭局域网

看着新操作系统的宣传广告天天不绝于耳，免费的新游戏一个接一个地在不停诱惑，计算机价格一天比一天跌得狠……手里的计算机却连看个电影都哆哆嗦嗦，很多人就只能向眉开眼笑的装机商拱手投降了。当新机落户后，老机该怎么办？当二手卖？价格便宜得让人心疼！送人？亲朋谁愿意成为垃圾回收站？

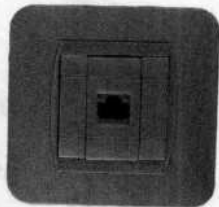
与其盘算再三，还不如动手在家里组建个小型局域网，让老机和新机共欢颜呢！在本章中，就将讲解如何在家庭通过各种方法实现小型局域网，以及如何在家庭局域网实现一些娱乐性应用！

4.1 家庭网络布线

在本节中，将讲解个人如何进行家庭网络布线，家居布线最注重美观，因此，布线施工应当与其它装修同时进行，要尽量将电缆管槽埋藏于地板或装饰板之下，信息插座也要选用内嵌式，将底盒埋藏于墙壁内。

4.1.1 布线基本知识

家庭布线分为装修前和装修后布线两种情况，装修前布线又分可以分为墙壁内置网线和未内置网线两种。如果开发商已经在墙壁里布下网线，那么只需购买如图所示的网线开关（也称五类信息模块）即可。



单口网线开关

信息插座的价格从十几元到一百几十元不等。根据经验来看，家用网络一般选择 20 元的产品就已经很好了。要统计信息插座购买的数量，一般使用如下计算公式：

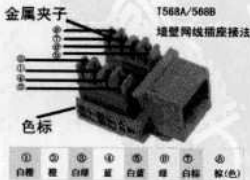
$M=n+n \times 3\%$

M：信息模块的总需求量

N：表示信息点的总量

n × 3%：表示富余量

插座里面的模块是可以拆卸的，拆卸后的模块如图所示。

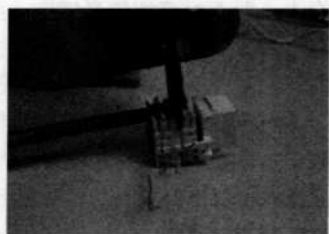


拆下的模块

在模块的两侧通常会有色标，根据这个色标可以轻松指引我们使用模块卡刀将双绞线压进去。把线剥开 40 厘米，把线分开放到网线模块的 8 个

第四章 组建家庭局域网

槽上，用卡刀把线逐根压下去，卡刀应该是刀刃那面朝外侧，这样可以自动把多余的线切断。



每根线对一个槽

压得时候用力要垂直，模块是很脆弱的，如果斜着用力模块容易裂开。听到“卡嗒”一声，就说明卡刀的凹槽已经将线芯压到位。把做好的信息模块按进面板的后面，会有锁扣自动卡牢。



压好的插座

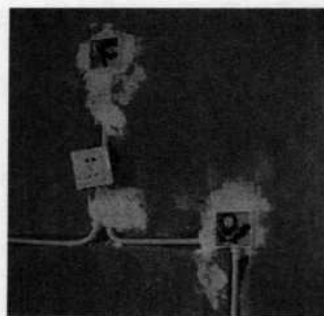
在向插座的凹槽中压线时，有几个比较常见的问题，即：

01 网线做线一定要按照568A或者568B吗？

答：不一定，其实网线的两头只要做成一样顺序就可以通。但是，这样做一来容易做错线序、二来是虽然可以通，但对传输距离可能有影响。不过一般家里的面积不大，这个问题不会有什么明显的影响。

02 墙壁上和地上的网线是直接用水泥压上吗？

答：不是的，通常会用一元多一米的PVC线管把线装进去，用水泥压住线管。这样，以后换线等维护操作起来就会非常的方便。通常，都是把网线和电话线放到一根线管中。



使用PVC线管

03 弱电和强电要离的很远吗？

答：家居布线中的弱电是指电视、电话、计算机网络、多媒体影音、安防报警等设备，因为这些设备与提供电能的系统不同，它们传输电压不高（一般在12V左右），故像这类线缆组成的系统我们称之为“弱电布线系统”。

强电产生的电磁场会对弱电信号有一定的影响。这两种线的确需要尽量避免平行的时候靠得太近，相对位置保持20CM左右即可。但是十字交叉是没有问题的，也是几乎无法避免的。

4.1.2 三室两厅布线实战

步入二十一世纪后，因特网已经和我们的生活密不可分，看新闻、玩游戏、欣赏电影、下载音乐……这一切都可以通过网络来完成。因此，在购买的新房中通常我们需要进行网络布线，让网络在房间中无所不在，实现网络化家居。

布置网线既可以聘请网络公司的人来做，也可以自己做。不要担心任务“繁重”，其实网络布线是非常简单的。关键在于懂得网线的走法（也就是拓扑）就不会有问题。

1. 信息插座的位置

在新居中布线对于很多人来说都是一个难题，因为好象一切从哪儿开始都显得非常茫然。其实，新居中布线是很容易的。首先，需要确认家具放在什么地方，家具位置无法确定就没有办法确定信息插座放在什么位置才好。所以，要做的第一件事就是把各个房间的长和宽画好画个草图或使



用圆方等家居系统设计一个比较正规的图纸。



在知道家具大概的位置和方向后，就好安排信息插座的位置了。比方说：

* 客厅

通常，在客厅的沙发边缘处会留一个信息插座，以便坐在沙发上使用计算机或将计算机放在沙发前的茶几上时使用。

* 卧室

很多家庭都不在卧室留信息插座，但是冬天在客厅和书房长时间用计算机看视频时，就会觉得在卧室里用计算机更舒服一些。所以，越来越多的人会买个床上计算机桌再放个笔记本电脑，选择在卧室使用计算机。由于主卧室通常会有两个主人，所以建议安装两个信息插座，以便双方能同时使用计算机。其它卧室和客厅只需安装一个信息插座，供孩子、客人或临时变更计算机使用地点时选用。卧室中的信息插座，一般都是位于床的两侧且不能被床遮住。

* 书房

书房一般需要留一个信息插座即可，如果需要多台计算机，可以买一个路由器。信息插座的位置一般会放在书桌的两侧，可以高于书桌。

* 餐厅

餐厅一般是不留信息插座的，因为一年到头也难得有个一回两回的会在餐厅用计算机，而且

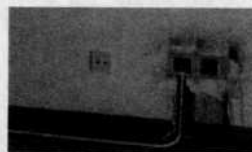
边吃饭、边用计算机也不利于健康。

* 阳台

在阳台上一般不推荐留信息插座，虽然也会偶尔兴起在这些地方使用计算机的念头——有些广告上会有“在阳台上边晒太阳边用笔记本电脑”的广告，不要相信这些“虚假”广告。因为在阳光下使用笔记本电脑，屏幕会很难看得清楚的。

知道了哪些位置需要放置信息插座后，接着，要确定 ADSL 准备放置的位置。因为所有房间都要从 ADSL 处引出相应的一条网线，这里就是所有房间的网线管理总入口。

如果 ADSL 是准备放在书房内，那么在书房那里就要有一个入户电话线插座，并用冲击钻在墙壁上打一个底盒槽，顺着底盒向下开一路宽 2.4 厘米、深度是 PVC 线管两倍（以便填充水泥）的线槽，将穿有网线的 PVC 管放进去。



规范的布线形式

在底盒中通常会有 4~6 条做好水晶头的网线伸出来，并与集线设备进行连接。一下子从墙壁里伸出这么多网线肯定不好看，所以，在布置家具时要考虑能有个书桌什么的挡住它。

水晶头的购买数量一般使用如下计算公式：

$$M = n \times 4 + n \times 4 \times 15\%$$

M：表示需要购买的水晶头总需求量；

N：表示信息插座的总量；

$n \times 4 \times 15\%$ ：表示留有的富余量。

2. 电话主插座的更换

为什么要谈电话主插座呢？这是因为家庭网络通常都是使用 ADSL 进行拨号上网的。电工在布线时，会把主电话插座（即含有入户电话线头和连接其它房间的电话线头）的几根线拧到一起。为了正确连接 ADSL，我们需要对这个主电话插座进行更换。具体方法是：

STEP 1 购买一个具有双电话接口的插座，

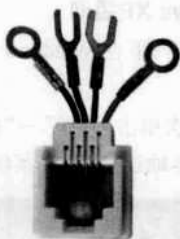
第四章 组建家庭局域网

价格一般在十几元。



双电话接口

STEP 2 拆下原来墙壁上的单口电话插座，将其中的几根电话线理开。将其中一根连接到电话插座的一个模块的接口上。

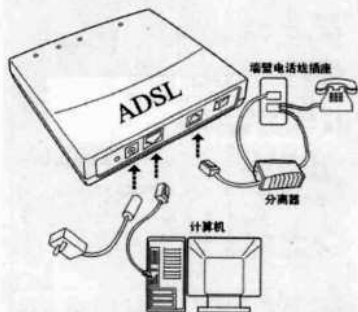


电话模块

STEP 3 将电话的话线水晶头插进去，拿起电话的话筒后发现没有信号则表示不是入户线头。更换插座上的其它线头，直至拿起话筒后发现信号，就表示找到了入户线头。

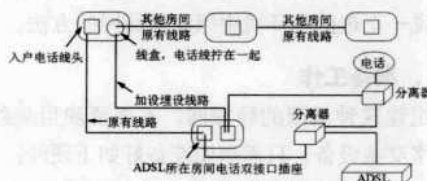
STEP 4 将入户线头外的其它线头拧到一起，并连接到电话插座的另一个接口上。接着，将电话插座安装到墙壁里的底盒内。

STEP 5 接下来需要按如图所示的线路图布线，这个是最基本的线路图，在这个基础上可以非常方便地更改线路。



网络布线

这里需要注意的地方有两点，一是如果 ADSL 不是放在电话主插座那里，而是放在另外一个房间的话。那么，从分离器中引出用于连接 ADSL 的电话线，可以从中剪断并加线延长到准备放置 ADSL 的房间。



电话入户线头和ADSL在不同房间

二是从 ADSL 中引出的网线既可以直接连接到一台计算机上，仅让这台计算机能够上网，也可以连接到集线器/交换机/路由器的某个 RJ-45 插槽中，如果是连接到集线器的话，那么，需要注意是否有 Uplink 端口，如果有就要插入到这个端口。如果没有 Uplink 端口，则表示所有的端口既可以当 Uplink 端口用，也可以当普通端口使用。

通过上述布线可以为各个房间内的计算机组建局域网，以及共享 Internet 提供基本硬件环境。



注意

如果小区预留有信息接口，那么布设一条从该接口到集线设备的双绞线，实现家庭网络与小区宽带的连接就可以了。

4.2 双机互联方案

很多人认识和学会组建局域网技术，都是从家用局域网组建开始的。在本章中，将分双机、三机和多机等几种不同规模和不同的操作系统环境，进行多种局域网组建技术的讲解。

双机也就是两台计算机，这样的局域网组建方法非常简单，也很多样化：如用串口、网卡、USB 联网线、IEEE 1394 接口、无线设备等等。在组建局域网时，需要牢记一条原则，即：根据实际情况选择最简单的解决方案，如果简单的方案能够解决问题，那么就不要用复杂的。



4.2.1 通过双绞线组网

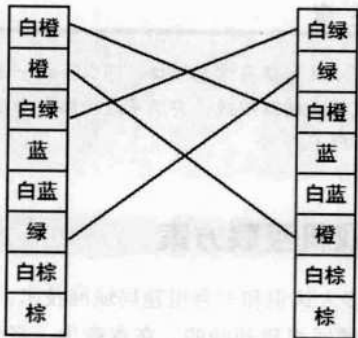
将两台计算机使用双绞线组建“直联”式（水晶头制作上是使用“交叉”法）局域网的技术非常简单、实用。由于目前 Windows XP 和 Vista 是家用计算机中安装最多的操作系统，所以，下面具体说一下这两种环境中组建局域网的方法。

1. 准备工作

- 组建这种类型的局域网，不需要使用集线器等网络交换设备，只需事先准备好如下硬件：
 - > 两台计算机分别准备一块以太网卡，速度使用 100Mbps 的就可以了。
 - > 双绞线一根，长度视具体情况定。
 - > 两个 RJ-45 水晶头，用于制作一根网线的两端接头，以便连接网线与网卡。

在完成硬件的选购工作后，接下来需要执行如下硬件设置：

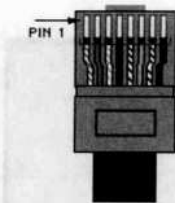
STEP 1 取一根所需长短的双绞线，将双绞线的一端外皮剥开，按从左到右的顺序排列双绞线，即：白绿、绿、白橙、蓝、白蓝、橙、白棕、棕；另一端的外皮也剥开，按从左到右顺序排列双绞线，即：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕。



交叉网线制作

上图中有两个交错重叠的叉形，这就是关键的地方。其中线 1、2 用于发送数据，线 3、6 用于接收数据，通过这样的连线制作就可以让两台计算机，通过网络进行数据收发了。这也就是为什么可以省却集线设备的原因。

STEP 2 使用压线钳把网线的两端制作好水晶头，要注意水晶头的方向是从左向右的。



水晶头方向

STEP 3 完成网卡的硬件安装，并将双绞线两端的水晶头分别插入两台计算机的网卡插槽。按下计算机主机上的电源开关，启动计算机进入 Windows 的桌面环境，根据提示完成网卡驱动安装。

2. Windows XP组网

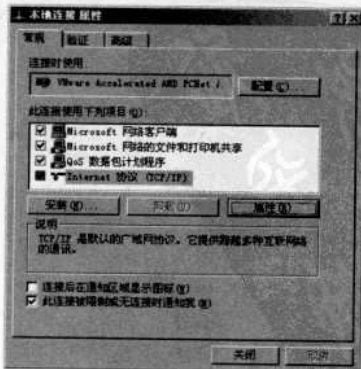
下面，讲解一下在 Windows XP 中的双机组网实现过程：

STEP 1 依次单击“开始”→“控制面板”→“网络连接”，右击“本地连接”并在菜单中选择“属性”。



在菜单中选择属性

STEP 2 打开“本地连接 属性”窗口，在列表中选择“Internet 协议 (TCP/IP)”项并单击“属性”按钮。

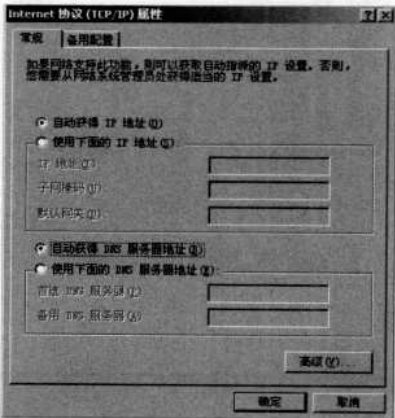


选择“Internet协议 (TCP/IP)”

第四章 组建家庭局域网

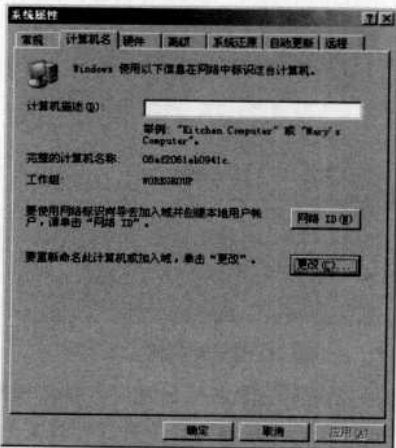
STEP 3 列表中的“Microsoft 网络的文件和打印机共享”项必须处于选中状态，这样才能保证两台计算机能看得见对方。

STEP 4 在打开的如图所示窗口中，这里的信息可以不必设置。因为 Windows XP 及以后版本的操作系统中，都支持多种模式的 IP 地址获得，这一点将会在本书以后的内容中讲解。此处略。



IP地址等信息设置

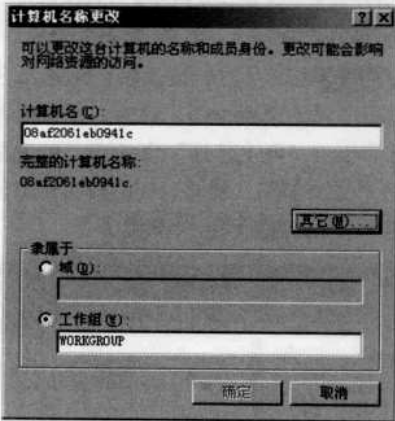
STEP 5 在桌面右键单击“我的电脑”，并在弹出的菜单中选择属性。在打开的“系统属性”窗口中单击“计算机名”选项卡，在切换到的界面中需要确认两台计算机是否使用相同的工作组名称（默认的名称都是“WORKGROUP”）。



计算机名称

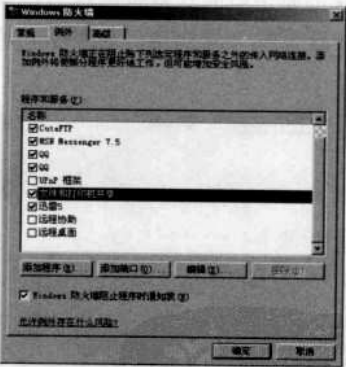
STEP 6 如果使用的工作组名称不同，则需

单击“更改”按钮并在弹出窗口中设置工作组名称为相同，我们可以根据喜好或工作需要修改工作组名称。在这里还可以为每台计算机起一个用于在网络中标识自己的名称，如“张三的机器”。



设置工作组名称

STEP 7 在“运行”栏中通过“Firewall.cpl”打开“Windows 防火墙”，在“例外”选项卡设置界面的“程序和服务”列表选中“文件和打印机共享”项，才能在防火墙中打开共享通道。



防火墙的设置

如果这里没有开放共享通道，则会在访问此计算机时出现如图所示的错误提示。



错误提示



注意

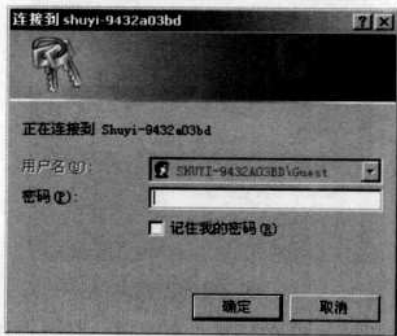
没有打开共享通道只会影响其它计算机对自己的访问，并不会影响自己对其它计算机的访问。

STEP 8 完成上述的设置后，在第二台计算机中进行同样的设置操作。此时，就可以在任意一台计算机的“网上邻居”窗口中，单击左侧的“查看工作组计算机”链接，在右侧窗格中切换到如图所示界面看到两台计算机了。



通过工作组找到其它计算机

STEP 9 在看到要访问的计算机后，默认设置下，双击要访问的计算机图标后会弹出一个登录框，这里默认只能使用来宾账户访问对方计算机。



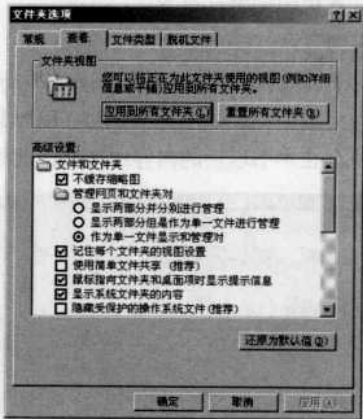
默认登录

之所以会出现这样的登录对话框，是因为服务器中使用了“简单共享”导致的。

因此，需要打开“我的电脑”窗口并依次单击“工具”→“文件夹选项”菜单，在打开的对话框中单击切换到“查看”选项卡，在这里需要取消“使用简单共享”项的勾选状态，

70

应用设置并建议重启系统后，即可出现能够输入账户名和密码的登录对话框。

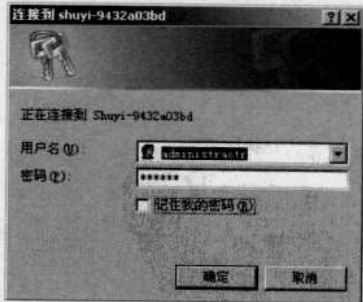


取消“简单共享”的勾选状态

注意

针对初级用户设计的“简单共享”让资源的共享操作非常容易，但有三个限制：一是无法进一步对资源进行各种定制；二是不允许设置 NTFS 访问权限（即不能出现“安全”选项卡）；三是简单共享方式只允许客户机通过 Guest 账户登录。

STEP 10 在出现下图登录对话框时，此时即可使用带有密码的账户登录到要访问的计算机中。



登录对话框

如果发现无论输入什么用户名和密码都是无效的，此时只有两种原因会导致这种情况出现：

一是使用的账户没有设置密码。这是因为组策略的“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”节点中，

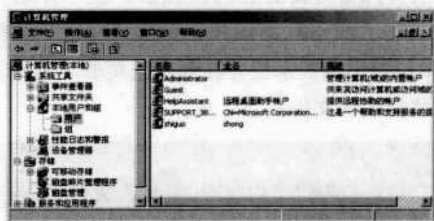
第四章 组建家庭局域网

“账户：使用空白密码的本地账户只允许进行控制台登录”项的默认状态为“已启用”所致。因此，解决这个问题的方法就是停用此策略即可。



停用策略

二是在“运行”栏中输入“Lusrmgr.msc”命令并按 Enter 键，在打开的“本地用户和组”窗口中，展开“本地用户和组（本地）”→“用户”项，在右侧用户列表中检查使用的登录账户名是否在“全名”一列中，如果是，则会出现此情况。



全名不能作为登录时使用

解决的方法是：在登录框中输入左侧“名称”列中的账户名和相应的密码，即可完成登录。下面解释一下“名称”和“全名”的意义：

* 名称：名称和全名都是用户账户的属性之一，用户名用来管理用户账户。在 Windows 内部是用 SID 来表示用户账户的，用户名可以说是 SID 的友好名称，类似于 IP 地址和域名的关系（网上邻居中登录指定的计算机时，要使用用户名而不是全名）。此外，这个名字还可以用来在没有欢迎屏幕的情况下登录系统，以及在给用户指定权限时用它选择用户或者在命令行中输入。

用户名可以包含但不能只由句号和空格组成，它最多可以包含除下列字符以外的 20 个大写或小写字母（用户名可以是中文）：

“/、[]:;|=, +*? <>”

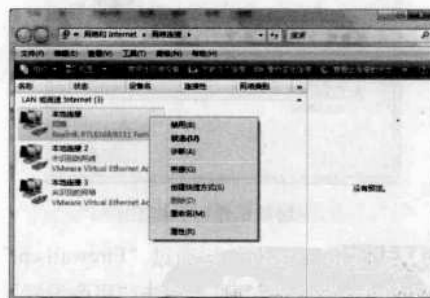
* 全名：全名用于在 Windows XP 的欢迎屏幕、“用户账户”窗口中和【开始】→“注销 ***”（星号即指全名）菜单中显示。全名可以在创建新用户时不输入，因为在创建中和创建后均可以随时输入。如果不输入全名，那么欢迎屏幕、“用户账户”窗口中和【开始】菜单中将显示“用户名”。

成功登录到要访问的计算机中后，就可以访问其中的相关共享资源。需要说明的是，上述一连串的访问限制实际上是可以绕开的。方法很简单，以 A 机访问 B 机为例，只需在 A 机中创建一个 B 机中有网络访问权限的账户（使用相同的密码），并使用这个账户进行 A 机登录，接着再使用“网上邻居”访问 B 机，即可实现无限制的访问了。

3. Vista组网

如果两台安装 Vista 的计算机需要临时组建局域网，在完成了本小节第一部分的硬件准备工作后，只需在两台计算机中执行如下操作即可：

STEP 1 在“运行”栏中使用命令“Ncpa.cpl”打开“网络连接”窗口，选中“本地连接”图标并单击鼠标右键，在弹出的菜单中选择“属性”项进入其属性窗口。



选择属性

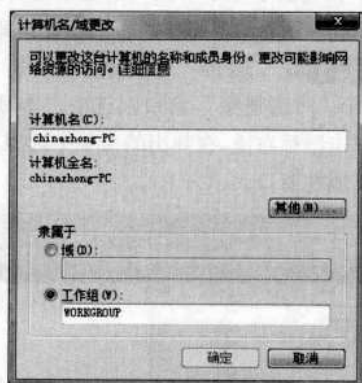
STEP 2 确认属性窗口的“此连接使用下列项目”列表中“Microsoft 网络的文件和打印机共享”项处于勾选状态后，选中“Internet 协议版本 4 (TCP/IPv4)”项并单击“属性”按钮。

STEP 3 在“搜索”栏输入命令“Sysdm.cpl”并按 Enter 键打开“系统属性”窗口，在“计算机名”选项卡界面中检查两台计算机的工作组名是否一致（如均为默认的“Work Group”）。



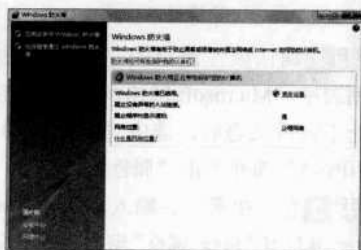
检查工作组名称

STEP 4 如果两台计算机的工作组名一致，可以直接单击“确定”按钮关闭属性窗口。如果两者不一致，应单击“更改”按钮并在弹出的对话框中，将其中的一台工作组名称更改为与另一台计算机的工作组名称相同，即便是工作组名称不一样也没关系，因为可以直接使用 IP 地址互访。



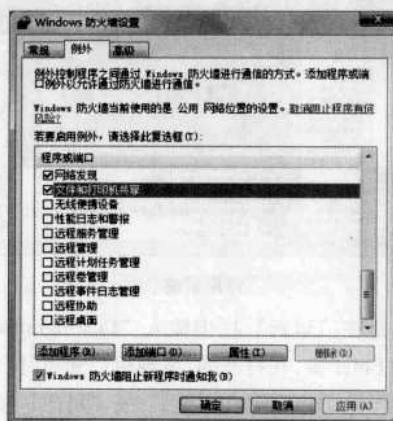
修改工作组名称

STEP 5 在“运行”栏通过“Firewall.cpl”打开“Windows 防火墙”窗口，单击“更改设置”项。



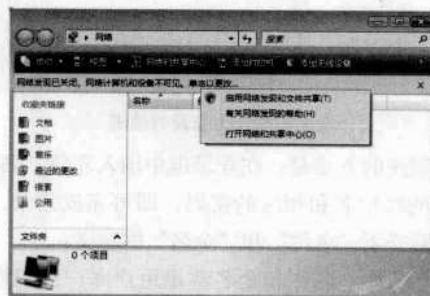
防火墙状态

STEP 6 在弹出的如图所示窗口中，要确认“例外”选项卡界面中“程序和服务”列表中的“文件和打印机共享”项处于勾选状态，这样才能在防火墙中开放共享通道。



更改防火墙设置

STEP 7 完成上述的设置后，在“开始”菜单中单击“网络”菜单并在弹出“网络”的窗口中，单击弹出的提示栏并在弹出的菜单中选择“启用网络发现和文件共享”项。



启用网络发现和文件共享

在这里我们遇到了一个新的名称“网络发现”。网络发现是一种网络设置，可以用于以下方面：

- > 启用此项后，方可允许网络上的其它计算机和设备看到或访问自己的计算机。

- > 启用此项后，方可访问网络中其它计算机上的共享设备和文件。

- > 根据连接到的网络位置，让系统协助提供合适的安全级别。

第四章 组建家庭局域网

在默认状态下，Vista 会禁用“网络发现”功能，因为需要在局域网中进行资源查看与访问，所以要启用此功能。在选择“启用网络发现和文件共享”项后，会弹出如图所示的对话框。

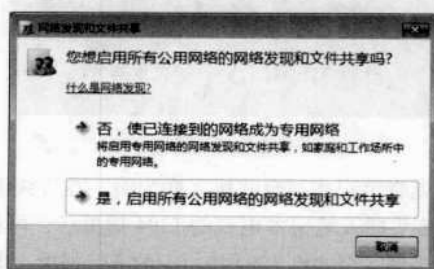


图 4-1-1 网络发现和文件共享对话框

这里有两个选项，其功能和作用分别如下：

> 否，使已连接到的网络成为专用网络。选择此项可以使当前计算机能够看到网络中的计算机与设备，同时使自己的计算机也可以被别的计算机发现。

> 是，启用所有公用网络的网络发现和文件共享。选择此项后将限制发现其它计算机和设备，并限制某些程序使用网络。如果网络上只有一台计算机并且无需共享文件或打印机，则最安全的选择是“公共场所”。此后，当计算机在公共场所连接到网络时，“公共场所”位置会阻止某些程序和服务运行，这样可以帮助保护计算机阻止未授权的访问。

在选择“是，启用所有公用网络的网络发现和文件共享”项后，“网络和共享中心”的“网络发现”和“文件共享”两项将自动被设置为“启用”状态。“Windows 防火墙”的例外列表中，将自动勾选“网络发现”、“文件和打印机共享”和“远程协助”三个项目。如果选择的是“否，使已连接到的网络成为专用网络”项，则会将防火墙中的配置永久更改为允许通讯。

这里的设置随时都可以在“网络和共享中心”中进行修改，方法很简单：单击“网络和共享中心”中的“自定义”按钮打开如图所示的窗口后，在这里即可进行修改。

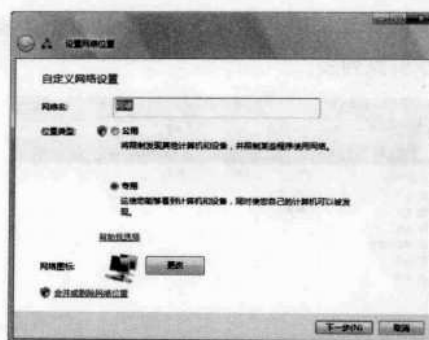


图 4-1-2 自定义网络位置对话框

单击“是，启用所有公用网络的网络发现和文件共享”项后，网络窗口中开始局域网中的计算机搜索工作，在地址栏中可以看到搜索进度。



图 4-1-3 网络窗口

在搜索的过程中，搜索到的计算机将会不断地被添加到右侧窗格的列表中。看到要访问的计算机后，双击要访问的计算机图标会弹出登录框。

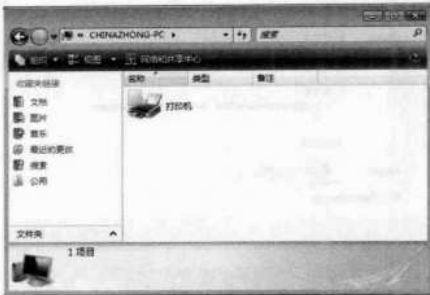


图 4-1-4 登录对话框

此时，必须输入“要访问的计算机”中具有网络访问权限的账户名称及其密码，方可登录到



要访问的计算机中，并且查看到该计算机中提供的共享资源列表。



访问共享资源

成功登录到要访问的计算机中后，就可以访问其中的相关共享资源了。

4.2.2 通过IEEE 1394组网

IEEE 1394 是一种传输速率可以达到 400Mbps 的高速接口，利用 IEEE 1394 技术除了可以完成外部设备与计算机之间的高速数据传输外，还可以通过 IEEE 1394 接口实现双机或是多机联网，这种联网方式的最大优点就是高速、稳定。在本小节中，将讲解如何在 Windows XP 中实现 IEEE 1394 方式的组网。

1. 准备工作

目前，IEEE 1394 接口有 4 针和 6 针两种，台式机通常是具有 4 针或 6 针接口的 IEEE 1394 接口卡（也有内置此接口的主板），而笔记本电脑通常会内置 1~2 个 4 针的 IEEE1394 接口。



1394卡和内置插槽

我们需要根据使用的 IEEE 1394 接口卡的不同（有四针和六针之分），选择相匹配的线缆。

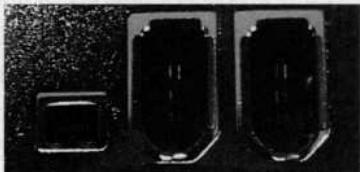


选择合适的线缆

以将笔记本与台式机互联为例，在将线缆的 4 针接头插入笔记本电脑的 1394 插槽后，再将 6 针接头插入台式机 1394 接口卡的 6 针插槽，即可完成硬件的连接。

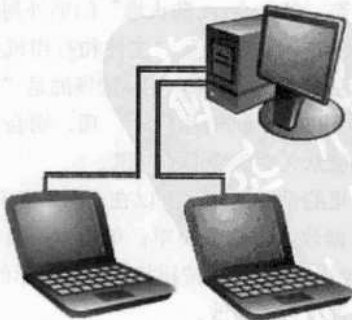
2. IEEE 1394网络概述

IEEE 1394 网络使用的是对等结构，不需要设置专门的服务器。因为 IEEE 1394 接口卡通常会提供 3 个或更多的 IEEE 1394 接口，所以，使用 IEEE 1394 接口组网不仅适用于双机互联，还适用于组建树状网络结构的多机互联。



同时具备多种类型的接口

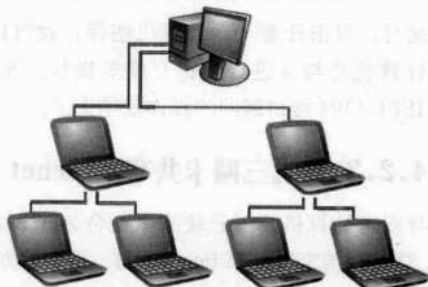
比方说，如果是使用带有 3 个接口的 IEEE 1394 接口卡，那么将每一个接口都与一台计算机相连，就可以轻松组建出多机互联的网络。



网络结构

第四章 组建家庭局域网

在此基础上，网络的规模还可以扩大。举例来说，一块 IEEE 1394 接口卡有 3 个接口，那么，就可以让当前计算机连接到 a、b、c 三台计算机，这样就是 4 台计算机的互联了。而 a、b、c 三台计算机如果每台再有三个 IEEE 1394 接口的话，那么，除了一个接口可以用于和上层连接外，另外两个接口还可以与另外两台计算机相连，树状的网络结构就是这样组建完成的。



无限扩张的网络

在这个树状结构中，整个网络将会以最理想的 400Mbps 速度运行。但 IEEE 1394 网络也有自己的致命伤，它要求网络中的每一台“上层”计算机都不能关闭，否则该计算机下面的所有计算机都将从网络中断开来。

3. 组网实战

通过执行如下操作，可以使用 IEEE 1394 方式实现双机的互联：

STEP 1 将 IEEE 1394 接口卡插入计算机的 PCI 插槽。



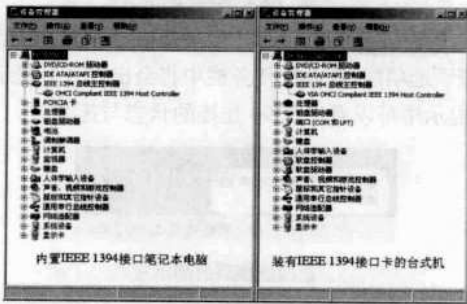
安装 IEEE 1394 接口卡

STEP 2 启动计算机并进入系统桌面后，系统会自动安装好该卡的驱动程序。如果是内置此插槽，则会在安装系统时自动安装好，故此步骤可以略。



发现新硬件和安装驱动完成

STEP 3 检查笔记本电脑与台式机的“设备管理器”对话框中是否存在 IEEE 1394 网络适配器和 IEEE 1394 控制器，如果存在则表示 IEEE 1394 设备已经正常安装。



检查硬件安装状态

STEP 4 分别打开两台计算机的“网络连接”对话框，检查其中的“1394 连接”是否已启用。



驱动安装后，自动出现相应图标

STEP 5 用鼠标右键单击“1394 连接”图标，并在弹出的菜单中选择属性。在打开“1394 连接属性”对话框后，确保有“Microsoft 网络客户端”、“Microsoft 网络的文件和打印机共享”和“Internet 协议 (TCP/IP)”这三项存在并勾选。



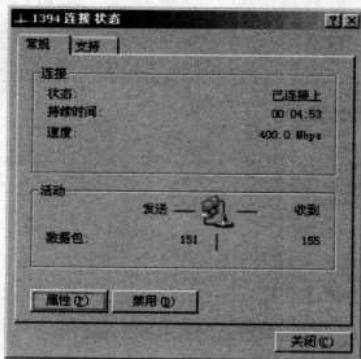
设置属性

STEP 6 单击勾选“连接后在通知区域显示图标”选项后，在系统任务栏中将会出现一个提示，从提示中可以看出 1394 连接的状态与速度。



已经连接后的提示

STEP 7 双击系统任务栏中的 1394 连接图标，在弹出的“1394 连接 状态”对话框中可以看到当前通过 IEEE 1394 方式收发的数据包量。



连接的工作状态

STEP 8 依次单击“开始”→“设置”→“网络连接”菜单，在弹出的“网络连接”对话框中单击左侧的“查看工作组电脑”项，稍待片刻就可以在右侧对话框中看到通过 IEEE 1394 方式联网的计算机的名称。



在工作组中看到所有计算机

此时，双击任意一台计算机图标，就可以进入该计算机并与其进行数据交换等操作。至此，通过 IEEE 1394 接口联网的操作就结束了。

4.2.3 双机三网卡共享Internet

将两台计算机通过三块网卡配合 ADSL 共享上网，这是目前家庭共享 Internet 的一种主流方式。这种方法成本低廉，实现过程非常简单。在本小节中，将讲解如何在 Windows XP 环境中实现双机共享 Internet 的任务。

1. 硬件设置

以 A 和 B 两台计算机组建“双机三网卡”式的局域网环境为例，需要执行如下操作：

STEP 1 在 A 机中先后（不要同时安装，以便区分网卡与“本地连接”的关系）完成两块网卡的硬件安装，在启动计算机后完成网卡的驱动安装。

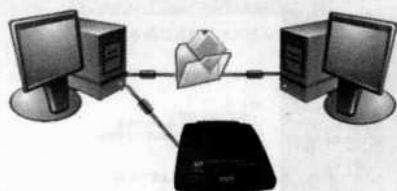
STEP 2 重启计算机后，打开“网络连接”窗口可以看到两个“本地连接”，第二块网卡名称后面会有升序的数字，如“本地连接 2”。



每块网卡对应一个“本地连接”

STEP 3 将其中一块网卡用与 B 机相连，第二块网卡与 ADSL 相连用于实现上网。

第四章 组建家庭局域网



硬件连接方式

2. 创建拨号连接

由于需要两台计算机共享 ADSL 上网，所以，应对装有两块网卡的 A 机进行 ADSL 的安装与设置。通过执行如下操作，可以完成 ADSL 的拨号连接的创建：

STEP 1 先参考本章前面的内容完成 ADSL 的硬件连接。

STEP 2 依次点击“开始”→“程序”→“附件”→“通讯”→“网络连接”，在弹出的窗口中单击左侧的“创建一个新连接”链接。



创建新连接

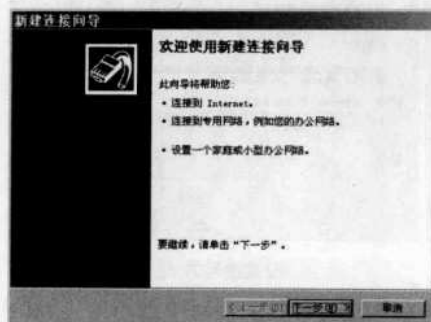
STEP 3 如果是第一次创建连接，会自动弹出一个需要输入位置信息的窗口。



设置所在地区信息

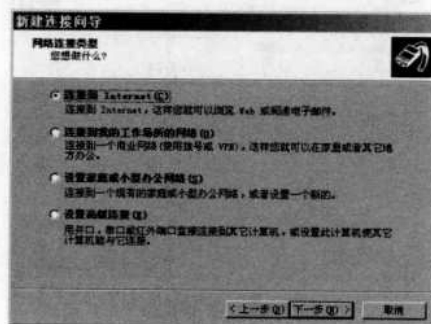
STEP 4 输入所在地区的电话区号并单击“确

定”按钮后，在弹出的“新建连接向导”窗口中单击“下一步”按钮继续。



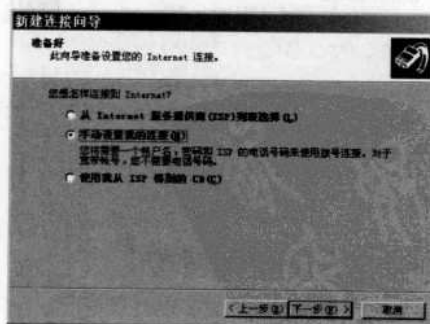
新建连接向导

STEP 5 随后弹出的“网络连接类型”窗口中共有四个选项，这里要选择第一项继续。



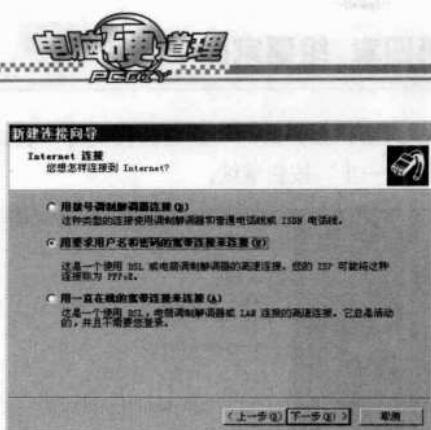
设置连接类型

STEP 6 再在弹出的“连接方式设定”窗口中，选择第二项“手动设置我的连接”继续。



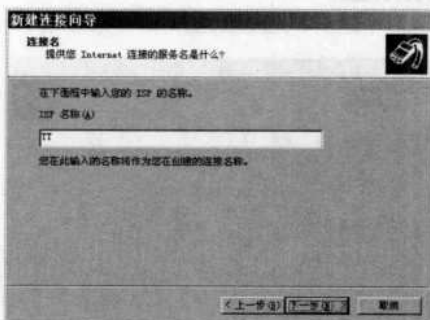
设置连接方式

STEP 7 接着出现如图所示的设置窗口中，选择“用要求用户名和密码的宽带连接来连接”选项继续。



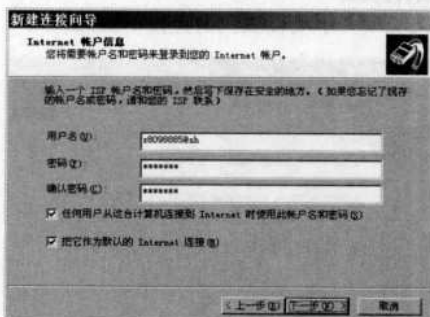
设置拨号方式

STEP 8 接下来的窗口中需要输入 ISP 的名称，这里的名称可以随便起，比方说“铁通”的网络起个“TT”也可以。



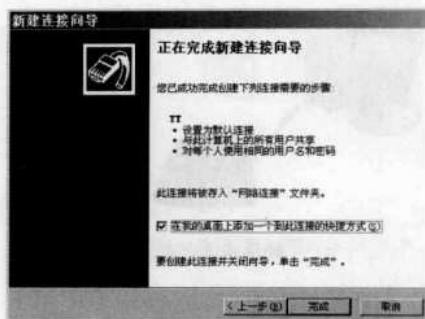
设置ISP名称

STEP 9 接着出现的窗口中要注意了，这里需要输入和 ISP 签订协议上给出的用户名和密码。



这里的信息不能错

STEP 10 在随后出现的完成界面中，选中“在我的桌面上添加一个此连接的快捷方式”项的单选框后，单击“下一步”按钮即可完成拨号连接的创建。



完成创建

STEP 11 稍后自动弹出连接拨号窗口后，窗口内的用户名和密码等内容均会自动添加完毕，我们只需单击“连接”按钮即可开始通过 ADSL 进行拨号了。拨号成功后就可以使用 IE 浏览器上网、通过 QQ 或 Messenger 程序进行网络聊天，以及进行更多的网络应用了。



拨号窗口

3. 共享Internet

本小节中，将讲解如何使用 Windows XP 的“Internet 连接共享 (ICS)”功能，实现双机共享 Internet。为此，需要执行如下操作：

STEP 1 在 A 机中依次单击“开始”→“控制面板”→“网络连接”菜单，打开“网络连接”窗口，选择用于连接 ADSL 的那块网卡（即“本地连接”）并单击右键，在弹出的菜单中选择“属性”。

第四章 组建家庭局域网



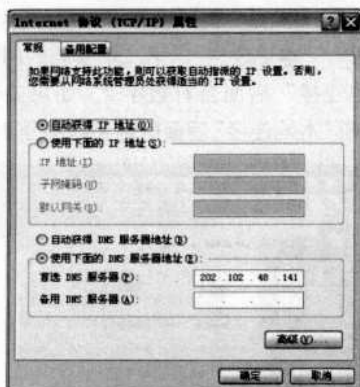
选择属性

STEP 2 在弹出的属性窗口中确认列表里的“Microsoft 网络客户端”、“Microsoft 网络的文件和打印机共享”和“Internet 协议 (TCP/IP)”三个选项处于选取状态。



设置属性

STEP 3 双击打开“Internet 协议 (TCP/IP)”属性对话框，在该对话框中选择“自动获得 IP 地址”，在 DNS 中设置 ISP 告之的 DNS 地址。



设置DNS信息

STEP 4 单击“确定”按钮返回上一步并切换到“高级”选项卡界面。在这里选中“允许其它网络用户通过此计算机的 Internet 连接来连接”等三个复选框。



激活共享上网选项

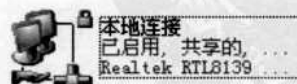


注意

Windows XP 自带防火墙支持多用户共享功能，这是一个很重要的优点。

STEP 5 在“家庭网络连接”列表中选择用于和 B 机连接的那块网卡，单击“确定”按钮后 Windows XP 将自动完成相关的设置。

STEP 6 返回到“网络连接”窗口后，与 ADSL 相连的网卡图标左下角将会出现“手”状的共享符号，右上角有“锁”状符号，这表示已经启动共享连接和处于防火墙保护下。

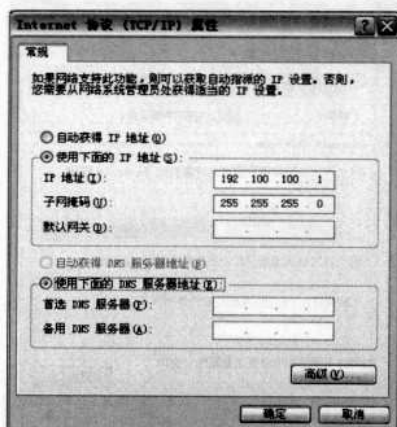


连接图标状态

STEP 7 在 A 机中右键单击连接局域网的那块网卡，在弹出的菜单中选择“属性”，在打开的对话框的项目列表中，确认“Microsoft 网络客户端”和“Internet 协议 (TCP/IP)”为选取状态。双击

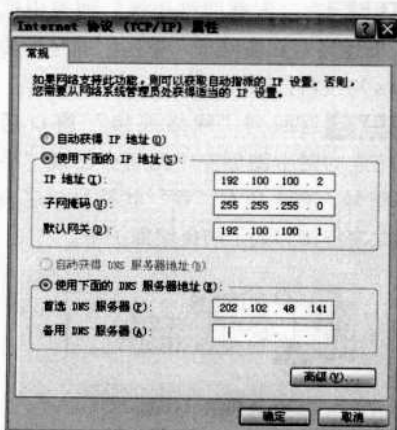


打开“Internet 协议 (TCP/IP)”属性对话框，在该对话框中指定 IP 地址为 ADSL 说明书中指定的默认网关地址，如 192.100.100.1，保持“默认网关”和“首选 DNS 服务器”为空。单击“确定”按钮后，即可完成 A 机的共享设置。



设置 IP 地址

STEP 8 在 B 机中打开“本地连接”属性窗口，双击进入“Internet 协议 (TCP/IP)”协议的“属性”按钮，在打开的对话框中单击“使用下面的 IP 地址”和“使用下面的 DNS 服务器地址”。在“IP 地址”中输入与 A 机同网段但不重复的 IP 地址，如 192.100.100.2。



设置网络

STEP 9 在“默认网关”中设置 ADSL 指定的 IP 网关地址，即 192.100.100.1；在“首选 DNS 服务器”中设置 ISP 指定的 DNS 地址。连续点击

❖ 80 ❖

“确定”按钮后，稍后设置即可生效。

此后，每当 A 机拨号上网成功后，B 机只需打开 IE 窗口就可以即刻上网了。至此，两台计算机就实现了“双机三网卡”的共享 ADSL 上网。

4.3 三机互联方案

三台计算机组建局域网也是很常见的。在本节中将讲解“三机四网卡”和“两根 USB 联网线”两种常见的三机互联方法。

4.3.1 使用三机四网卡实现互联

作为一种相对廉价、易行的三机组网方式，“三机四网卡”方式还是很值得向大家推荐使用的。本组网方案的硬件与软件环境如下：

> 在 A 机中安装了两块网卡，其余计算机各安装一块网卡；

> 所有计算机的操作系统均为 Windows XP。

1. 准备工作

首先，需要在 A 机中安装两块以太网卡，分别用于连接 B 机和 C 机。安装网卡时，需要注意网卡要先一块并连接到 B 机，然后再装一块连接到 C 机。不能同时安装，否则容易搞混淆。

此外，两块网卡在硬件安装要注意最好隔一个或多个 PCI 插槽，也就是说，如果 A 网卡安装在了第一个 PCI 插槽中，那么就将 B 网卡安装在第三个 PCI 插槽中，避免网卡之间有可能出现的硬件冲突，虽然在理论上这样安装并无问题。

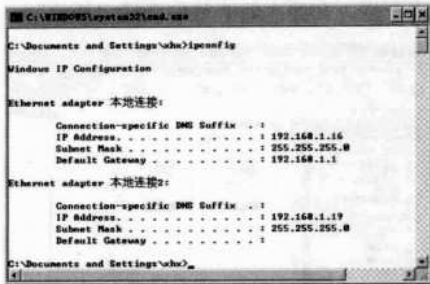
在完成安装后，就可以在“网络连接”窗口中看到两个“本地连接”，第二块安装的网卡对应的“本地连接”后面会有数字 2。如果安装更多的网卡，则“本地连接”后面的数字就会是 3、4……



安装双网卡后

第四章 组建家庭局域网

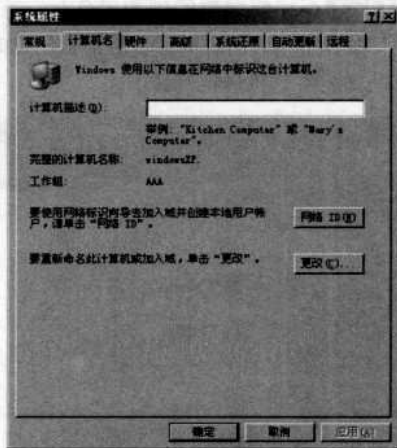
如果在“命令提示符”窗口中使用命令“IPconfig”的话，则会看到如图所示的两个 IP 地址信息。



检测IP地址

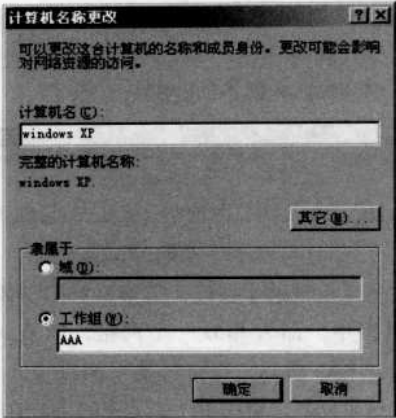
这两个 IP 地址分别对应了两块网卡，IP 地址既可以自动获得，也可以手工进行输入设置。

三台计算机中需要设置工作组一致的名称，以及设置每台计算机的名称为不一样，即：在桌面上用鼠标右键单击“我的电脑”图标，在弹出的菜单中选择“属性”。在弹出的“系统属性”对话框中单击切换到“计算机名”选项卡界面，并单击下方的“更改”按钮。



查看工作组名称

稍后，在弹出的“计算机名称更改”对话框中，分别在三台计算机中设置“计算机名”为不同，设置“工作组”名称为相同的，如“AAA”。



设置工作组名称计算机名称

设置完毕后，单击“确定”按钮重新启动计算机。此时将两根使用“交叉法”制作好的直联式网线将 A 机中的两块网卡各连接一台计算机。



连接示意图

2. 网上邻居的不同之处

完成三台计算机的连接后，三台计算机之间的网络环境是不同的，即：

在 A 机的“网上邻居”窗口中，可以同时看到三台计算机的存在。这意味着在 A 机的“网上邻居”中，可以立即对 B、C 两台计算机进行访问。



网上邻居



在 B 和 C 两台计算机中，将只能看到本机和 A 机两台计算机存在，如果试图访问另外一台计算机，则会弹出类似于如图所示的错误。



访问错误

之所以出现这个错误，因为 B 和 C 分别处在一个网络中，即 A 和 B 一个网络，以及 A 和 C 另一个网络。所以，B 和 C 是不能直接互访的。要解决这个问题，请见下一小节中的解决方案。

3. 使用网桥功能

什么是网桥？网桥是一种能够实现两个网络相互连接的设计。网桥不仅可以用于连接网络，还可以在整个网络负载较大的时候对网络进行切分，从而控制网络流量。所以使用网桥连接网络，可以有效避免扩展网络时引发的速度减慢问题。

在 Windows XP 中的任一计算机里，当安装了两块网卡并分别连接到一个网络时，就可以使用网桥技术将两个网络连接到一起。



网桥连接

通常，网桥具有如下的作用：

- > 可以扩展网络的长度，增加网络的规模。
- > 减少由于网络规模扩大而导致的流量问题。
- > 两端可以连接不同的物理介质。

网桥工作在 OSI 模型的数据链路层，它可以检查流经网桥的每个数据包的源和目的地址，可以在传递信息的时候，根据已经在网络上发送过数据的计算机地址创建路由表，根据该信息，网桥就可以知道哪些计算机位于哪些网段中。

网桥配置简单，成本低廉，因此适合应用到一些中小规模的网络中。在本小节中，配置网桥的方法如下：

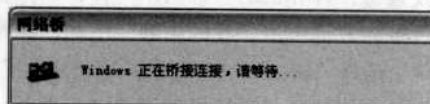
STEP 1 在安装了两块网卡的 A 机中，打开“网络连接”窗口。

STEP 2 选中要进行桥接的两个“本地连接”并单击右键，在弹出的菜单中选择“桥接”。



创建网桥

STEP 3 随即将会自动开始网桥的创建，此时要停止其它的操作。



创建网桥

STEP 4 在完成网桥的创建操作后，在“网络连接”窗口中就会出现网络桥的图标。此时，B 机就可以直接和 C 机进行互访了。



桥接图标

STEP 5 右键单击“网络桥”图标并在弹出的菜单中选择“属性”，可以设置绑定在网桥上的协议和服务。如，可以添加或删除网卡，也就是从网桥中添加或删除某个网络。

第四章 组建家庭局域网



网桥属性

由于在一台计算机上只能创建一个网桥，所以，只能将多个网络连接添加到一个网桥中，而不能试图创建多个网桥环境。



注意

如果在计算机的某个网络连接上启用了 Internet 连接共享特性，或是激活了 Internet 连接防火墙，这时该网络连接将不用被配置为网桥的一部分，同样，在该网络连接的快捷菜单中也不会出现“添加到桥”的菜单命令。

4.3.2 使用USB联网线组网

使用 USB 联网线组网是一种很方便的组建局域网技术，在本小节中将讲解如何在 Windows XP 中使用两根 USB 联网线实现三机互联的方法。

1. 准备工作

USB 联网线两端都采用了标准的 USB 接口，中间多了一个“包”，其核心功能就在这个“包”中——里面有一块网络芯片用来实现联机功能。

在购买 USB 联网线时要注意不要错买了只有拷贝功能的 USB 连机线，USB 联网线的功能是：

既具有拷贝功能，又具有网络功能，作用相当于两块网卡。

使用 USB 联网线组网至少有以下几点优势：

> 功能强。完全实现普通以太网的功能(文件、设备和打印共享、Internet 接入共享、联机游戏等)。

> 价格低廉。两根 USB 联网线也不过区区几十元，而正常情况下，3 台计算机的 3 块 8139 网卡就已经是 120 元了。

> 容易实现。USB 接口已十分普及，目前无论台式机还是笔记本电脑基本上都具备该接口。

> 不需拆机。使用 USB 联网线时不用打开机箱大动干戈，而且 USB 技术本身就支持热插拔，可随时灵活地变动连接对象。

2. 组网实战

使用 USB 联网线组网的整个过程是非常简单的，首先，需要在 3 台计算机中分别安装好 USB 联网线的驱动程序，这样才能让 USB 联网线虚拟出的网卡可以正常工作起来。下面，以 Windows XP 系统为例讲解一下安装“鹏宏 USB110”联网线驱动程序的方法：

STEP 1 在 USB 联网线附赠的驱动程序光盘中找到“net driver”文件夹，双击其中的“Setup”程序运行驱动安装向导。如果在安装过程中出现“没有通过 Windows 徽标测试”这样的提示框，不必理会它，直接单击“仍然继续”按钮继续安装即可。



注意

USB 联网线大多会同时配置直接电缆连接驱动程序和网络功能驱动程序，请注意这两种驱动程序是不一样的，只有后者才能让 USB 联网线实现虚拟网卡功能。

STEP 2 驱动程序安装完毕后，无需重启 Windows XP 即可在“网络连接”对话框中看到虚拟的“网卡”已经安装好了，只不过因网线未连接，所以显示出“网络电缆被拔出”的提示。



网络安装成功

STEP 3 将 USB 联网线插入计算机的 USB 接口后，在弹出的“发现新硬件”对话框中单击“下一步”按钮，系统将会自动识别硬件（即 USB 联网线中部的“包”）并为其做好使用前的准备工作。

在完成驱动的安装后，因为网络协议在安装 USB 联网线时就会自动安装好，所以，此时只需确保所有电脑中的工作组名称相同就可以了。不同的操作系统中设置工作组的方法前面已经详述过，这里就不再重复了。

接着，需要将两根 USB 联网线的一头分别插入两台电脑的 USB 接口，再将这两根 USB 联网线的另一头分别插入第三台电脑的两个 USB 接口中，就可以完成硬件连接了。



连接方式

在完成硬件的连接后，就可以在三台电脑中打开“网上邻居”对话框，进行三机的互访了。

使用这种方法联网，不足之处在于 USB 联网线的价格还有点贵，优势在于现在计算机的 USB 插槽大多都有 4-8 个，所以只要联网线数量够，那么网络的扩展就显得非常容易。

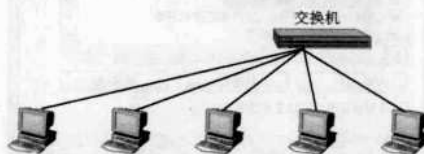
4.4 带路由 ADSL+交换机多机共享

多机互联就是将多台计算机建成局域网，目前，多机互联可以使用集线器、交换机、路由器、

无线 AP……等设备实现。下面，将从家庭多台计算机使用交换机组网的角度出发，讲解如何进一步实现多机共享 Internet 的应用。

4.4.1 准备工作

使用交换机组网，需要先把交换机的位置确定，因为所有计算机都需要从交换机那里引线。



使用交换机组网

当交换机的位置确定下来后，还需要根据每台计算机的位置，计算出所需的网线长度（每根网线要额外加 1-2 米）。为了节省网线，交换机的位置最好能处于网络的中部——合理的交换机位置可以在一定程度上减少网线的浪费。



注意

必须将网线多留一些，因为水晶头往往会因为各种原因而损坏，这时就需要重新制作接头了。如果网线留得过短，将会很麻烦。

在根据计算机的数量用“1 机 × 2 个接头”的方法算出所需的水晶头数量后，因为利用交换机组建的局域网，网线的两端接头的做法是一样的。所以，网线每端的双绞线顺序依次为：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕。

这是最容易犯错的地方，很多人直接将白绿线与绿线相邻放在一起，这样将会造成信号的串扰，使局域网传输效率降低、数据流出现易断等现象。所以，新手信在这方面要注意了。

网线接头制作完毕后，就可以完成本节组网前的准备工作了。

4.4.2 ADSL 设置

带路由功能的 ADSL 可以本身完成拨号及上网信号的地址分发工作，由于产品面板上并未提

第四章 组建家庭局域网

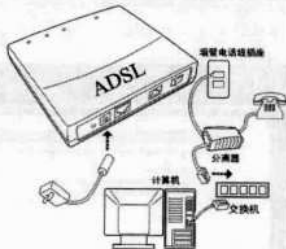
供有多余的 LAN 接口，即是不具备交换功能，所以，如果选用这类设备共享上网，需要再选购一台交换机用于连接网内所有的计算机。

要使用带路由的 ADSL+ 普通交换机实现 Internet 共享上网，需要执行如下操作：

STEP 1 将每台计算机与交换机之间，都使用网线连接起来，并确认交换机至少还有一个空槽，以便连接 ADSL 时使用。

STEP 2 参考本章 4.2.1 小节中的内容完成网络协议方面的设置，实现局域网的组建。

STEP 3 将 ADSL 上的网线插入交换机的任意一个 RJ45 插槽。



连接示意图

STEP 4 由于 ADSL 内置了拨号功能，所以，需要参考 ADSL 说明书将计算机的 IP 地址等信息完成设置。只有设置默认网关和 IP 地址为指定范围（即与 ADSL 的 IP 地址为同一网段），才能访问 ADSL 的管理页面。

STEP 5 打开一个 IE 浏览器并在地址栏中输入 ADSL 的 IP 地址，如“http://192.168.1.1”，在按下 Enter 键后将会打开类似于如图所示的管理页面。



ADSL 管理功能登录页面

STEP 6 根据 ADSL 说明书上的提示完成账户名和密码的输入后，单击“确定”按钮进入 ADSL 管理页面。通常需要在 WAN 管理界面中设

置“封装协议”为 PPPoE，并输入 ISP 给的上网账户名和密码。



设置拨号信息



注意

这里的 VPI 和 VCI 信息每个地方是不同的，这一点可以参考一下其它用户的 ADSL 设置。

在保存设置信息并重启 ADSL 后，设置信息将立即生效：开始自动拨号上网了。看到 ADSL 的黄灯停止闪烁后，就可以在连接到交换机的每台计算机中打开 IE 浏览器进行网络应用了。

4.5 非路由 ADSL+路由器共享

现在为了防止用户一号多机上网现象发生，一些 ISP 提供的 ADSL 都是没有提供路由和拨号功能的。本小节将讲解如何使用带有管理功能的路由器，配合这类 ADSL 实现多机 Internet 共享。

4.5.1 准备工作

使用不带路由功能的 ADSL，通常只能在计算机中创建拨号连接（创建拨号连接的过程请见本章前面的内容）进行拨号操作。因此，要想实现硬件自动拨号，只能购买一个具有拨号功能的宽带路由器。

在硬件连接方面，和 4.4 节中讲解的方法是一样的。不同之处在于带有宽带功能的路由器价格相对于普通交换机贵上一些，以及 ADSL 的网线必须插入到路由器的 WAN 端口，而计算机的网线必须插入到 LAN 端口中。



连接示意图

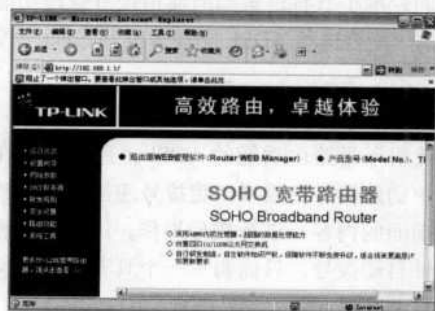
目前，支持宽带的路由器大多提供了简体中文的配置，以及提供多方面的管理功能，比方说，可以具备 DHCP、虚拟服务器、DMZ 主机、防火墙、上网权限管理、静态路由表、UPnP 等管理功能，等等。所以，不必担心不会设置。

4.5.2 路由器设置

使用支持拨号的宽带路由器配合 ADSL，是将计算机中的发送拨号连接的信号改成由路由器发送拨号信号。因此，需要在路由器中进行拨号信息的输入。下面，以一款 TP-Link 路由器为例，进行的设置如下：

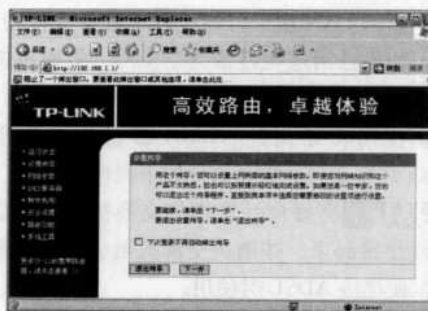
STEP 1 根据路由器说明书的要求，将连接路由器的计算机 IP 地址、默认网关更改为要求的范围，即同一网段。

STEP 2 打开 IE 浏览器并在地址栏中输入路由器 IP 地址，如“http://192.168.1.1”，按下回车键后完成登录并进入类似于如图的管理页面。



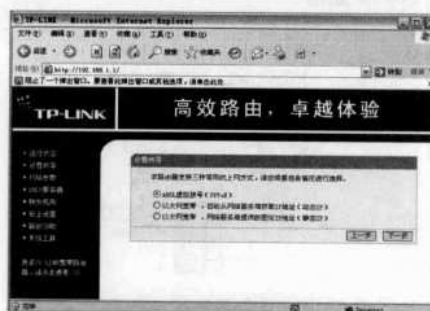
路由器管理功能首页

STEP 3 单击左侧的“设置向导”，在右侧切换到的界面中可以看到通过向导设置拨号信息非常容易，使用向导功能配置拨号信息一般只需两、三个步骤就可以了。



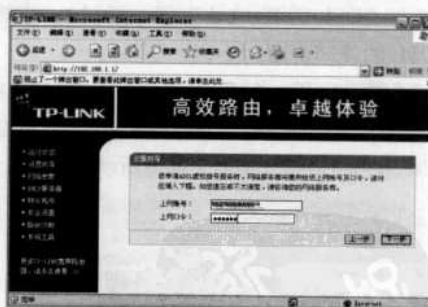
向导说明页面

STEP 4 单击“下一步”进入如图所示的页面后，一般需要选择第一种拨号方式。



设置拨号方式

STEP 5 单击“下一步”按钮进入如图所示的页面后，在这里输入 ISP 给的用户名称和密码。

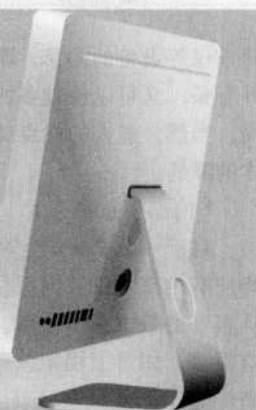


输入账户信息

STEP 6 单击“下一步”按钮进入页面后，单击“完成”按钮即可结束设置任务。

STEP 7 此时重启路由器即可让其自动配合 ADSL 发送拨号请求，拨号成功以后的 ADSL 黄灯会停止闪烁。此时，即可让局域网中的任意计算机上网浏览了。

第五章 组建中小型企业网络



越来越多的企业意识到了电子商务（EC，即“E-Commerce”的缩写）的重要性与无限商机。越来越多的企业发现企业内部使用电脑化管理将会使工作效率大幅攀升。的确，随着经济全球化和电子商务的到来，企业如果还固守于传统模式，必定将不能适应这种经济发展的趋势。

如今，大多数的企业都已经使用计算机进行各类办公，并使用内部局域网完成企业内的各种交流。在本章中，将讲解如何在中小型企业中实现内部局域网。

5.1 企业局域网概述

中小型局域网可以使企业在建立起灵活、高效、宽松、可靠的网络化办公环境的同时，还采用 TCP/IP 技术与互联网之间架起一座桥梁。内外网络的开通，可以让企业的信息交流与共享、对外展示企业形象、宣传和发布产品信息等方面全面提升档次，进而保持与客户、合作伙伴的亲密联系。

越来越多的企业，都意识到使用网络除了可以提高工作效率外，还可以对企业的发展有着积极的作用，如：

- > 提高部门间协作的效率；
- > 存取、共享各种资料非常方便；
- > 可以共享大量硬件设备，进而有效节省办公费用支出；
- > 提升电脑的安全级别；
- > 积累大量潜在的用户；
- > 网络是广告宣传的另一种有效传播方式；
- > 可以展开高效的电子商务。

5.1.1 功能及特点

中小企业通常是指规模在 500 人以下的企业，

如果进一步细分，又可以分为 100 人以下的小型企业，100-250 人的中小型企业，250 人以上中型企业。中小型企业网络的功能跟其它网络有一定的区别，它的功能和特点如下：

1. 企业局域网的基本功能

网络作为企业的一个窗口，已经成为企业运作中一个不可或缺的发展平台。特别是企业与客户的互动环境，更是让企业欣喜不已，企业的局域网绝不是摆设，它能给企业真正带来效益，是企业经营的需要，是一种战略投资！

作为企业级办公局域网来说，应该具有以下的基本功能：

* 共享功能

通过组建局域网，可以实现数据和设备的共享，这是局域网最大的优点。在以前乃至当今，有许许多多的办公部门还是用一个或多个文件柜作为文件的存储设备，在调用某些资料时就只能翻箱倒柜，逐份查找，耗时耗力之弊端显而易见。如果配备了计算机，那么该机用户调用文件时连开机和找到文件往往只需数分钟即可。如果配备了局域网，那么，所有人查找资料都可以非常方便。

从硬件共享这个角度来看，打印机、刻录机、



扫描仪等设备的共享，既可以使管理变得更加井井有条，又可以使设备的利用率得到大幅度的提高。当然，最大的优点还是可以实现硬件采购成本的降低。

* 内部服务器

对于一个重视安全管理的企业办公网络来说，均应有内部专供数据保存的服务器，这样可以起到很好的数据备份作用。一个企业要保存的数据有很多，如员工档案、财务报表、进销数据的备份等等。

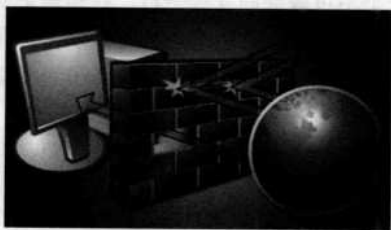
如果还有架设邮件服务器的话，还可以最大程度地避免企业信息的外泄，通过邮件窃取商业机密这已经是不争的事实。

* 远程访问和 VPN

路由和远程访问服务 (Routing and Remote Access Service) 可以让远程用户连接到企业的局域网，VPN (Virtual Private Network, 虚拟专用网) 可以让远程用户通过 Internet 安全地访问企业内部的网络资源，比方说调用自己办公室的计算机中的数据等等。

* 防火墙功能

防火墙 (Firewall) 能够在网络与电脑之间建立一道监控屏障，保护在防火墙内部的系统不受网络黑客的攻击。



防火墙的位置

逻辑上讲，防火墙既是信息分离器、限制器，也是信息分析器，它可以有效地对局域网和 Internet 之间的任何活动进行监控，从而保证局域网内部或单机的安全。

* 网络的可扩展性

随着企业规模的扩大，设计的企业网络应该能够允许网管方便地进行新设备的添加，因此，应尽量选用可堆叠或模块化产品，因为它们具有

很好的开放性，可以十分方便地扩充网络的容量。如 D-Link DES-1024D 交换机通过 MDI/MDIX 上行链路端口，就可以进行轻松的网络扩展，通过该端口可以把几台交换机级联到一起获得更多的端口。

当一个局域网能够提供上述功能时，从一定程度上说，就可以满足大多数中小型企业的需求了。

2. 企业局域网的特点

在中小型企业中，使用的网络结构、设备、操作系统等都是不一样的，下面简单地谈谈两种不同规模的局域网特点。

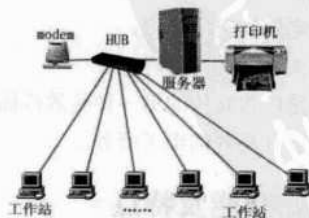
所谓小型局域网，一般是指由 50 台以下计算机互联组成的网络系统。其主要应用是办公、文件和打印共享、共享上网、企业内部管理应用（如财务管理、进销存管理、客户关系管理等）等。组建小型局域网的方案有多种，目前大部分都集中在 100MBit/s 快速以太网方案，快速以太网由于其采用了集线器或交换机堆叠，因此其具有较好的扩展性能，能轻易扩展到高达 100 个节点的网络环境。而其高速度的数据交换、数据存储为小型企业提供了一种高性能的网络平台。本节以 100Base TX 为标准组建小型快速企业以太网。



注意

目前快速以太网分为 100Base TX、100Base F X、100Base T4 和 100Base T2 四种（“T”表示双绞线，“X”表示快速，“F”表示光纤）。

在节点设备较少或没有特殊需要的情况下，小型企业局域网可采用集线器或堆叠交换机来实现 100Base TX 网络互连，此时整个网络系统结构。



小型 100Base TX 星型结构

第五章 组建中小型企业网络

小型企业局域网建设的基本需求是经济、实用、高效、有一定的扩展空间。因此，在设备的选购上要精心选购，尽量达到高性价比的需求。

所谓中型局域网，是指联网计算机数量在50～150左右的网络。在此规模的网络环境中，需要采用两级网络结构，增加主干交换。这种两级的网络结构，由高性能的主干交换机和连接计算机的二级交换机构成。网络服务器连接在主干交换机上，联网计算机通过二级交换机的上连端口，从主干线上访问网络服务器。中型局域网广泛应用于办公、教育、流通等中小型局域网环境（或中大型网络主干）的日常办公、多媒体教学等。

5.1.2 企业布线须知

在设计企业网络结构时，要考虑其成本、扩充性、安装维护是否方便，等等。在企业网络建设中，布线可以说是真正的一次性投资，人们很难以追加投资的方式来提高它的性能。因此，技术人员应当对布线知识有个较熟练的掌握。

布线的正规名称是“建筑物综合布线系统”（Premises Distribution System, PDS），它是在计算机技术和通信技术发展的基础上，进一步适应社会信息化和国际上融入化的需要，也是办公自动化进一步发展的结果。作为建筑技术和信息技术相结合的产物，布线已经成为网络技术人员的必备技能之一。

1. 布线原则

布线系统的性能在很大程度上决定了网络的使用性能，所以布线系统的规划应以目前所能达到的尽可能高的性能为标准。故而，在布线时应当遵守以下几个原则：

* 走线整齐美观

试想走线零乱的布线现场必将带给人一种混乱的感觉，正规的走线应在有条件的情况下在墙壁内的布线；无条件的也应使用穿线管将网线井井有条地固定在墙壁的中下部，当然这样网线的实际使用长度要远远超出走线零乱的网线长度了，无疑会增加很多成本的支出，但是从办公便利性的角度来看，这还是值得的。

* 保留适当长度

不要将网线在交换机与电脑网卡两端的长度只留一点点，正确的做法是应保留一定活动的余地，比方说办公桌的移动、水晶头的脱落，都需要有一定长度的网线。试想，水晶头与网线的连接必需重做时，网线只有短短的10几厘米长，那么显然将会在重制水晶头连接时带来制作上的一些麻烦。正确的做法是在两端都保留半米至一米的长度。

* 保持适当弯度

综合布线是有标准可循，我国相关标准有GB50311/GB50312、EIA/TIA 568B ISO/IEC等。它们对双绞线的折弯度是有严格要求的，有些看上去整齐的布线，折弯度却并不符合布线标准。

* 不要与市电并在一起

在本书的内容中多次讲到，弱电和强电之间不要放在一起，可是很多时候都会在布线时出此类的问题。



强弱电要分离

2. 企业布线设备

企业布线和家庭布线有很多不同之处，如在交换设备、传输介质、管材等方面的选用上都可以看出这一点。下面，以管材为例谈谈相关的选用经验。

在布线系统中，管材是一个非常重要的组成部分，在这上面的花费比较多，因为需要尽量选用材质优良的产品，有些管材要能经受得住风雪雨阳的考验才行，不能用一段时间后，碰一下就散了架。

管材的种类有金属槽、PVC槽、金属管、PVC管等，金属槽价格较贵但经久耐用，在企业布线中常使用的尺寸有：50×100mm、100×100mm、100×200mm、100×300mm、200×



400mm 等。

金属管布线一般适用于室内、外场所，但对金属管有严重腐蚀的场所不宜采用。

PVC 槽一般在室内使用，从规格上讲有：20 × 12 mm、25 × 12.5 mm、25 × 25 mm、30 × 15 mm、40 × 20 mm 等。与 PVC 槽配套使用的附件有很多，如阳角、阴角、直转角、平三通、左三通、右三通等等。

表：配套附件

阳角		阴角	
直转角		平三通	
顶三通		左三通	
右三通		连接头	

3. 布线要点

在进行企业布线时，有一些要点是需要注意的，如：

- > 线缆通常会高出地面 2.2M 以上。
- > 垂直敷设时，每隔 1.5 米左右就要进行一次固定。
- > 穿插在线管里的线缆一般不能捆扎，否则以后维护换线时非常麻烦。
- > 在管材交叉的地方要使用三通等“桥架设备”，以便维护线路时方便拆卸。
- > 信息插座一般距离地面 30 厘米以上。
- > 信息插座不要离计算机设备距离太远，以节省所用线缆。

5.2 网络设计方案

在制定企业办公室网络方案的时候，需要考虑到网络的实际使用情况，并且从硬件设备、网络结构类型以及操作系统等多方面来确定方案。

5.2.1 中心节点的选择

组建中小型企业办公局域网时，因为有一部

❖ 90 ❖

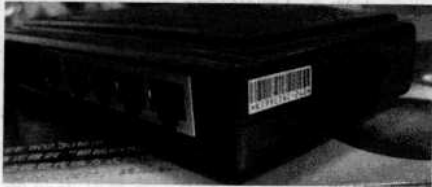
分硬件的选用与普通家用的硬件选择是一样的，这些内容读者们可以参考本书前面章节的内容。所以，下面针对企业网络谈一下关键硬件：中心节点的选择要点。

在星型网络中，中心节点是整个网络的心脏部位。由于网络中每一个节点向其它节点发送的数据都必须经过中央节点才能送达，所以，一旦中心节点出了问题，就会导致整个网络都无法正常工作，因此建议中心节点的选择一定要慎之又慎才行。

在目前的企业网络中，一般都是使用“交换机+路由器”作为企业网络中的中央节点。其中，交换机主要在各个部门内部使用，路由器则放在机房负责连接各个部门的交换机以及连接 Internet。



在选购部门交换机时，每个部门要根据人数来确定交换机的类型。比方说，领导基本上都是一人一个房间，那么为房间配置一个 4~5 口的桌面型百兆以太网交换机就可以了，自己用和来几个带笔记本电脑的客人也都够用，如图所示是 TP-LINK TL-SF1005D 这款交换机，价格在 50 元左右。



桌面型百兆以太网交换机

第五章 组建中小企业网络

现在，很多小型企业组网的时候都使用这样的“傻瓜”式交换机，因为这种交换机不需任何配置，与集线器一样，接上电源、插好网线就可以正常工作。

如果是部门使用的交换机，则需要先对部门工作人员人数做一个统计，在为每个人都留一个端口的同时，力争还能富余几个端口。这样，可以方便外部门的人员过来进行临时的数据交互。通常，使用 D-Link DES-1016D 这样的三百元左右的具有十六个端口的交换机就可以满足需求了。



十六口交换机

D-Link DES-1016D 采用了双层设计，它具备 16 个 10~100Mbps 自适应端口，通过前面板的 LED 灯可以清楚的看到 16 个端口的工作状态，便于用户十分方便的了解整个网络的环境。此外，此交换机还支持 VPN 功能并内置了防火墙功能，能够支持 TCP/IP、DHCP、ICMP、NAT、PPPoE、SNTP 等协议。

对于中型规模的企业局域网来说，通常会在楼层安装一个千兆以太网中心交换机，然后再由此交换机连接楼层中各个部门的百兆交换机。这样的交换机通常具有网管、VLAN 等功能，如 D-Link DES-1226G 等等。

DES-1226G 带有两个千兆端口，24 个百兆口，可以让企业的用户端使用百兆网络的基础上，通过千兆端口实现服务器的高速访问，所有的端口均支持自动线序交叉。作为智能型千兆交换机，DES-1226G 具有中央控制、自动触发功能，以及具有 8.8Gbps 背板带宽，6K MAC 地址空间，512K 帧缓存，支持存储转发，端口聚合，CRC 校验削减错误帧，支持帧长为 1518 Byte 的数据帧传输等特性。



注意

在经费允许的情况下，在企业网络中配备一台高性能的 UPS，可以为服务器、网络设备等带来莫大的益处，比方说在硬盘的保护和数据的紧急保存上，有时就远远超出 UPS 的本身价值了。

在中小型企业的网络设备中，核心路由器是所有内部不同子网之间通信的通道，也是整个网络的对外出口，是整个网络的重中之重。此外，网管还可以通过路由器管理网络。所以，应采用高安全、高可靠、高性能的高端路由器。



企业路由器

假设，现在有一个小型企业网络共有 50 台计算机，网管希望购买的路由器能够实现：能屏蔽部分网站、能屏蔽网络聊天及网络游戏、能在指定时间段才可以上网、能支持双线路接入等功能。能够满足要求的路由器比较多，关键看企业准备的资金有多少，比方说，资金充裕就买 Cisco 2800 系列路由器，否则就买一些杂牌路由器也可以，因为 50 台计算机的负荷对企业路由器来显得很小。

企业级路由器在买回后，在使用之前均需要进行大量的配置工作。因此，配置页面是否简单、功能是否强大，这些因素也建议在购买时当场测试一下，满意、学会后再买不迟，毕竟这些设备都是要花费几千、上万的费用。



注意

在网络建设中，布线可以说是真正的一次性投资，人们难以追加投资的方式来提高它的性能。布线系统的性能在很大程度上决定了网络的使用性能，所以布线系统的规划应以目前所能达到的尽可能高的性能为标准。



5.2.2 操作系统的选择

在企业网络中，操作系统的选择要面向应用、面向需要，充分利用现有资源，结合应用和需要的变化，制定出相应的方案，不要一味追求高、新、难，避免使用不成熟的技术，而且某些过渡时期的技术很可能导致网络建设的失败。

目前，可以使用的操作系统种类繁多，除 Windows 之外还有 UNIX、Linux 和 Novell 等，虽然它们在稳定性和安全性方面有着非常不错的表现，但对于普通用户来说，这些明显属于专业性很强的操作系统，一般用户还很难掌握在这些操作系统中配置网络和管理维护网络的方法。所以我们推荐大家使用以下的 Windows 操作系统组合。

由于办公室一般都是采用了服务器/客户端的组网方式，同时对于网络系统的稳定性、安全性和传输速度等方面的要求都很高。所以，建议在服务器中使用 Windows Server 2003 系统，在客户端可以安装 Windows 2000、Windows XP 或 Vista。

目前，主流的配置是 Windows Server 2003 R2 SP2+Windows XP PRO SP3，这种操作系统的配合既满足了服务器提供强大、完善服务的需求，也适应了客户端计算机用户要求简单、安全的需求，很适合在中小型企业或者办公室使用。

至于 Linux + Windows XP 的配合虽然也是相当不错，但是服务器的设置技术对于大多数的网管来说，都需要重新学习，不利于中小企业的网管快速上手。

5.2.3 TCP/IP 方案设计

在企业网络组建中，网络分布在几栋建筑物是经常遇到的问题，企业网络的分散性会给组网和管理带来了一定的难度。假设，某个企业在两栋楼中分别有数十台计算机，通常我们应该为两栋楼分别分配一个子网，也就是说，让两个子网来组成一个企业局域网。在进行这种规模的企业局域网时，我们应知晓以下几个方面的知识：

一是确定内部网 IP 地址的类型。我们都知道，IP 地址由 32 位二进制数字组成，8 位为一组，共有 4 组，中间用“.”隔开。每个 IP 地址有两部分，

即网络标识和主机标识，这两种标识长度的不同，使 IP 地址可以分为 5 类，常用的有 A、B、C 三类，相应的地址范围为：

A 类：1.x.x.x-126.x.x.x //X 表示 0-255 之间的任意数；

B 类：128.x.x.x-191.x.x.x；

C 类：192.x.x.x-223.x.x.x。

从上述分类不难看出，A 类 IP 地址表示少数网络上有众多主机；B 类 IP 地址表示网络和主机分布适中；C 类 IP 地址表示很多网络上有少量主机。在选择内部网的 IP 地址类型时，应根据内部网中的子网数量及每个子网的规模进行选择。在此选用 C 类 IP 地址，该地址的前 3 段标识不同的网络，第 4 段标识一个网络中的不同主机。为使 IP 地址反映内部网的特点，我们给其中每段都赋予了实际意义。第 1、2 段用来区分网络号，我们选择 192.168，这也是几乎所有局域网都选用的网络号；第 3 段区分不同地址位置的子网，如甲楼选择 1（即 192.168.1.x），乙楼选 2（即 192.168.2.x）。当内部网进行扩展时，有新的子网加入时，其 IP 地址的规划就显得很容易实现了。

二是客户机 IP 地址的分配。我们知道，内部网中的每一台计算机都是以 IP 地址标识网络位置的，因此在组建局域网之前，就要为所有的设备，如服务器、工作站等等分配好一个 IP 地址才行。其中客户机的 IP 地址分配由于数量较大，所以分配的方法就要灵活运用。通常，我们可以使用两种方式安排客户机的 IP 地址，一种是通过 DHCP 服务器来动态分配；另外一种是根据部门位置分配静态 IP。为了管理简单，推荐尽量采用动态 IP 分配的形式。如果一定要分配静态 IP，具体规划时就应尽量考虑使主机标识体现出内部网中客户机的某些特征，如所属的行政单位或所在具体物理位置等。如财务科的 IP 地址是 192.168.1.x；研发部的 IP 地址是 192.168.2.x；售后部的 IP 地址是 192.168.3.x。

5.2.4 中型网络设计案例

通常，我们把计算机数量在 150~500 台的企业网络定义为中型网络，中型网络跟小型网络不

第五章 组建中小型企业网络

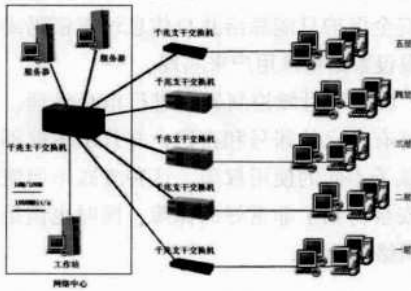
仅仅在规模上有所不同，安全性要求以及网络稳定性的要求相对来说也要高很多。

比方说，由于中型企业局域网规模比较大，因此可将其划分为主干网和分支网。目前，主干网的数据传输速率可为 100MB-1000MB，分支网的数据传输速率可为 100MBit/s，即当前主流的“主干千兆位，百兆位交换到桌面”。本节将结合具有典型意义的实例来介绍一些常见中型企业局域网硬件架构方案。

实例一：集中式网络

目前，大多数中小型企业都采用集中式办公方式，即所有部门和人员都在同一座建筑内办公。由于规模的限制，此种网络节点间的距离大都小于 100M，因此，采用超 5 类非屏蔽双绞线是此类网络布线的首选。例如：

A 公司是一个中等规模的企业，该企业在同一栋 5 层的大楼中。其中在 1~5 层共有 200 个计算机节点。网络中心与各楼层之间全部采用了超 5 类 UTP 建立 1000Base TX 高速网络，接入层采用了 10M/100M 自适应交换到桌面。其网络中心采用了高端口密度的千兆位主干交换机，各楼层之间采用了千兆位支干交换机，服务器安装了 1000MB 网卡。



集中式中型企业局域网结构

由于采用可堆叠交换机，因此网络的扩展性很强，可以根据企业的发展来增加新模块和堆叠交换机的数量，且随着端口和堆叠数量的增加，其总量拥有成本低的优势就越明显。

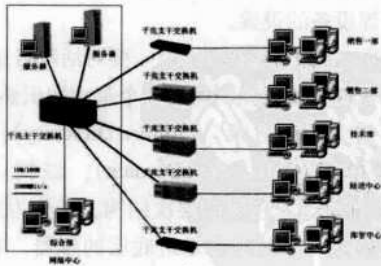
从图中可以看出，集中式网络通常包括网络中心和楼层多分布设备两层结构。网络中心交换

机可采用千兆位交换技术构成高速骨干，以连接服务器和楼层接入设备。中心交换机应具有大容量的交换模块，采用模块化机箱设计，可以支持多种速率和介质，而且端口密度高且扩展灵活。楼层接入交换机应具有千兆位上传端口，能够通过堆叠或增加模块来提高接入端口速度，还应当提供支持 SNMP 等网管协议，以便通过网络对所有设备的状况进行监控和管理。

实例二：分布式网络

分布式办公是指企业在一个园区内具有多处办公地点，楼宇网络的连接距离通常大于 100m，所以需要采用光纤进行布线。分布式网络通常具有网络中心及楼宇接入节点两个层次，当楼宇规模较大时，还会出现第三个层次：楼宇设备间。例如：

B 公司是一个具有多个部门的中型企业，该公司的不同部门分布于工业园区内的不同建筑中，由于各建筑与网络中心之间的距离小于 500M，故采用基于多模光纤传输的 1000Base SX 建立千兆位主干。中心千兆位交换机可安装 100/1000Base T 千兆位铜缆模块以连接服务器，另需选配 1000Base SX 模块以连接四座建筑，还可选配 10/100Base TX 模块实现本建筑内的接入。该方案采用光纤网络扩大网络覆盖范围，当连接超过 500M 时，则可选用单模 1000Base LX 长波光纤千兆位光纤技术实现 5KM 内的网络数据传输，该公司的网络拓扑如图所示。



分布式中型企业局域网拓扑

如果企业用于网络建设上的资金充裕，那么推荐在网络出口处使用硬件防火墙和路由器。

5.3 组建域模式局域网

对于要求比较高的企业来说，必须采用服务器/客户端方式组建局域网。在经费允许的情况下，将网站、DHCP 等各种服务由多台独立的服务器来完成最为适宜。这样可以实现各种服务之间的最大程度的独立性，即便有一台服务器崩溃了，其它服务器也可以正常运作。但是，如果经费不允许多台服务器的话，那么，也可以只由一台服务器来完成所有服务的提供。



下面，我们将学习基于“域”的、Windows Server 2003 标准主从式结构的多机局域网组建方法。

5.3.1 基本知识

首先，要明白在组建企业局域网时，要做的工作顺序是：先把计算机调试后，然后根据计算机的所在位置进行布线，最后才是服务器、UPS、防火墙等设备的设置。

其次，在服务器的调试中，要对活动目录、域、域树、域森林和域控制器这几个基本知识熟悉。

所谓“活动目录”（Active Directory），是指由组织单元（OU）、域（Domain）、域树（Tree）和森林（Forest）构成的层次结构。域作为最基本的管理单元，它同时也是最底层的容器，它可以对员工、电脑等基本数据进行存储。在一个活动目录中可以根据需要建立多个域。比方说，甲公司的财务科、人事科和销售科就可以各建一个域，因为这几个域同属甲公司，所以就可以将这几个域构成一棵域树并交给域树管理，这棵域树就是

甲公司。又因为甲公司和乙公司及丙公司都归 A 集团所有，那么为了让 A 集团可以更好地管理这 3 家子公司，就可以将这 3 家公司的域树集中起来组成域森林（即 A 集团）。显然 A 集团可以按“子公司（域树）→部门→员工”的方式进行层次分明的管理。活动目录这种层次结构使企业网络具有极强的扩展性，便于组织、管理及目录定位。

在域模式下，至少有一台服务器负责每一台连入网络的电脑和员工的验证工作，相当于一个单位的门卫一样，称为“域控制器（Domain Controller，简称为 DC）”。

域控制器中包含了这个域的用户账户、密码和属于这个域的电脑等信息构成的数据库。当电脑连入网络时，域控制器首先要鉴别这台电脑是否是属于这个域，用户使用的登录账号是否存在、密码是否正确。如果以上信息不正确，域控制器就拒绝该用户从这台电脑登录。不能登录，用户就不能访问服务器上有权限保护的资源，只能以对等网用户的方式访问 Windows 共享的资源，这样就一定程度上保护了网络上的资源。

其实域和工作组在结构上很相似，只是表现形式有些不同：

> 工作组：只能将数量不多的电脑连成一个可互相共享资源的网络，在这种工作方式下，信息的安全保护只能靠给共享信息设置密码或将使用权限设置给特殊用户来实现。

> 域：采用域控制器来进行信息管理，每个用户都有自己的账号和密码，并且可根据不同的情况赋予不同的使用权限，这种方式不但使网络信息安全得到了非常好的保障，同时也满足了大中型网络的要求。

5.3.2 组网实战

域模式的局域网组建任务，主要就是架设一台具有域控制器功能的服务器，接着再将使用不同操作系统的工作站登录或加入到域的操作过程。所以，整个操作过程是由服务器端和客户端分别设置构成的。

1. 服务器端设置

首先，请读者们参考本书前面的内容完成

第五章 组建中小型企业网络

Windows Server 2003 的安装，具体过程此处略。

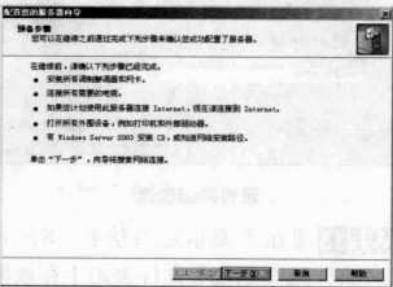
接着，需要在 Windows Server 2003 中安装活动目录，因为系统中附带了活动目录的安装向导，所以，我们能够在它的帮助下，快速将一台普通服务器设置为域控制器，并且可以在没有连接到网络时预先设置 DNS 服务。具体的设置过程如下：

STEP 1 依次单击“开始”→“程序”→“管理工具”→“管理您的服务器”菜单项，弹出“管理您的服务器”对话框。



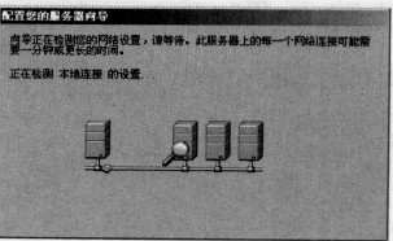
服务器管理功能

STEP 2 单击“添加或删除角色”后，将出现服务器配置向导界面。



配置界面

STEP 3 单击“下一步”按钮后，将出现“配置您的服务器向导”界面。



检测设置

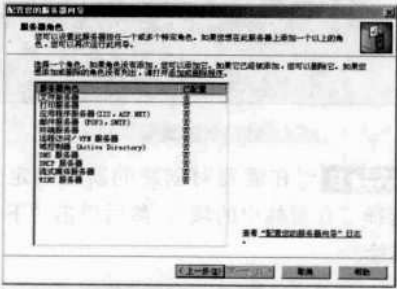
STEP 4 稍待片刻后，将出现“配置选项”

界面，单击“自定义配置”及“下一步”按钮继续。



配置选项

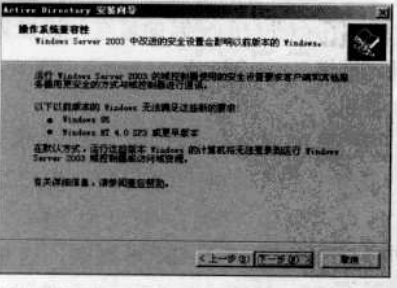
STEP 5 在出现的“服务器角色”列表中，可以看到“域控制器 (Active Directory)”项的后面是“否”，这表示该服务还没有安装，请选择该服务，并单击“下一步”按钮继续。



服务器角色

STEP 6 在弹出的欢迎对话框中，将告之下面将运行 Active Directory 安装向导来将此服务器设置为域服务器，这里可以直接单击“下一步”按钮，进入 Active Directory 安装向导界面。

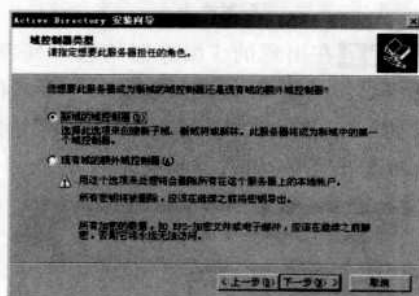
STEP 7 这时，可以从对话框中了解一些有关活动目录的安装要点与注意事项。接着单击“下一步”按钮进入“操作系统兼容性”提示界面中。



注意事项

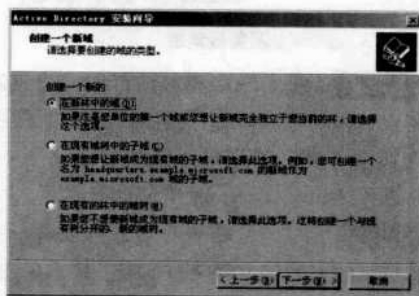


STEP 8 在下一步中需要设置域控制器的类型。这里有两种域控制器类型：新域的域控制器和现有域的额外域控制器。请注意，如果网络中没有现成的域控制器，应该选择“新域的域控制器”项，此时服务器将成为新域中第一个域控制器，要是网络中已经有了一个或多个域控制器，就应该选择“现有域的额外域控制器”项，这样服务器将以域的形式加入到现有的域控制器中。以只有一个域控制器为例，这里采用前一种方式来安装域控制器。



域控制器类型

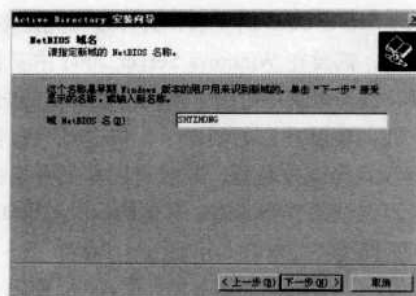
STEP 9 现在需要对创建的新域确定类型，这里选择“在新林中的域”，然后单击“下一步”按钮继续。



创建新域

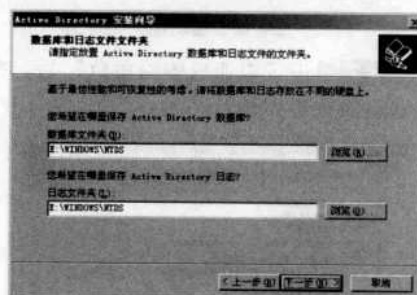
STEP 10 在进入的“新的域名”设置界面中输入新域的域名，如“shyzhong.com”，然后单击“下一步”按钮。

STEP 11 在下一步出现的“NetBIOS 域名”设置界面中，由于早期的 Windows 用户是采用 NetBIOS 域名来标识域的，所以为了向下兼容，在这里可以命名一个 NetBIOS 域名，这里输入“SHYZHONG”，然后单击“下一步”按钮。



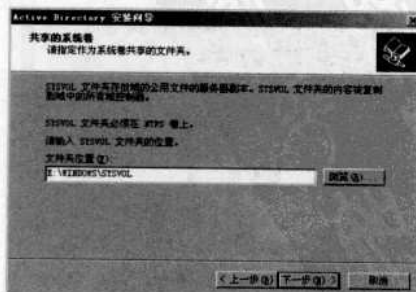
设置 NetBIOS 域名

STEP 12 现在需要指定活动目录的数据库和日志文件存放位置。基于最佳性能和可恢复性的考虑，最好将活动目录的数据库和日志文件放在不同的硬盘分区上，此时可以在相应的对话框中分别输入数据库和日志文件的存放位置，也可以通过右边的“浏览”按钮来确定存放的位置。然后继续单击“下一步”按钮。



设置存储位置

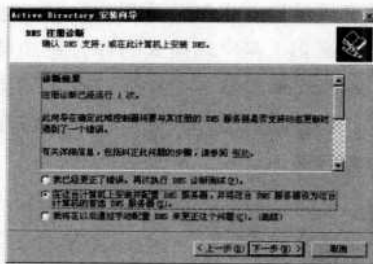
STEP 13 现在需要指定系统卷 (Sysvol) 共享的文件夹。这个系统卷文件夹用于存放域的公用文件副本，其中的内容将会被复制到域中的所有域控制器。在这里可以自行定义文件夹的位置，不过要求必需放在 NTFS 分区中。



设置路径

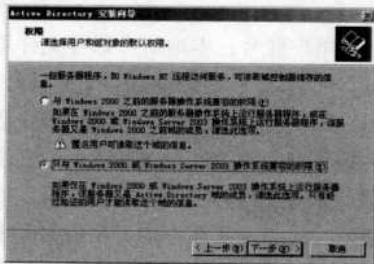
第五章 组建中小型企业网络

STEP14 在进入配置 DNS 服务器的界面后，如果服务器还没有配置 DNS 服务器，那么在安装活动目录的同时可以顺便进行 DNS 服务器的配置。此时建议用户选择“在这台计算机上安装和配置 DNS 服务器……”项，省得以后还要重新对其进行配置。



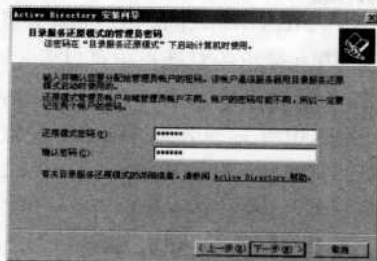
配置选项

STEP15 在随后出现的界面中，需要根据组建域（包括服务器和客户端）的操作系统类型来选择相关选项。



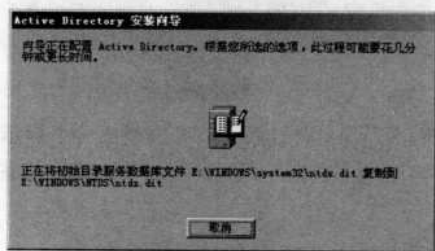
设置权限

STEP16 下一步需要设置目录服务还原模式的管理员密码，该密码主要是在系统从“目录服务还原模式”下启动时使用的，它与登录服务器时所使用的系统管理员账号有所不同。在对话框中输入两个完全一致的密码后继续。



设置密码

STEP17 在出现的摘要对话框中，系统会把前面所有的设置项目内容逐一列表显示出来，检查无误之后即可进入 Windows Server 2003 系统对活动目录的配置过程，根据当前硬件配置的档次高低不等，这个过程可能会需要花费 10 分钟左右的时间，所以请耐心等待一会儿。



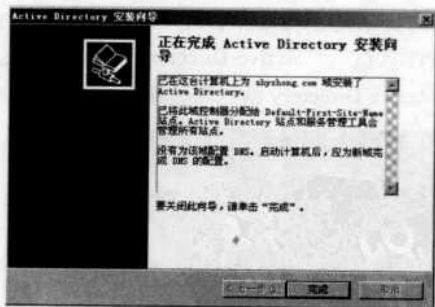
开始配置



注意

请在进行配置之前，将 Windows Server 2003 安装光盘放入光驱中，以备配置向导进行安装文件的调用。

STEP18 配置过程结束后，会弹出活动目录已经安装配置完成的提示。最后，根据系统提示重新启动电脑，这样就完成了活动目录的整个安装配置过程。



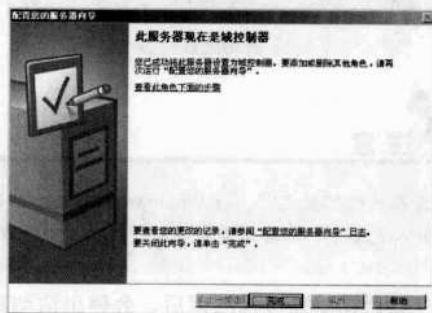
完成配置

STEP19 重新启动服务器后，在登录框中需要输入正确的用户名和密码后，才能进入名为“SHYZHONG”的域服务器。



登录对话框

STEP 20 在登录系统后将会弹出一个提示框，告之当前的电脑已经是域控制器了。单击“完成”按钮关闭提示框。



完成设置

STEP 21 依次单击“开始”→“设置”→“控制面板”→“管理工具”菜单，从中找到3个有关活动目录的管理工具，即“Active Directory 用户和计算机”、“Active Directory 域和信任关系”和“Active Directory 站点和服务”。



新增的菜单

其中，第一个工具主要是对活动目录中的用户、电脑、用户组和其它内容进行管理，另外两

个工具则分别用于管理域之间的信任关系和创建站点及活动目录中的相关信息。对于普通的域网络环境来说，“Active Directory 用户和计算机”工具最为关键，所以下面就重点来看看这部分内容。

安装好 Windows Server 2003 中的活动目录之后，如果想让网络中的其它电脑能够登录到服务器，就必须给这些电脑分配用户账号，这样才能构建出服务器 / 客户端模式的办公室局域网。在 Windows Server 2003 中提供了几种不同类型的用户账号，分别是内置用户账号、域用户账号和本地用户账号等。



注意

内置用户账号：安装 Windows Server 2003 时，由系统自动创建的账号称为内置账号。**域用户账号：**域用户账号允许用户登录到域中，并且可以访问网络中任意位置的资源。

本地用户账号：本地用户账号允许用户登录服务器，并且访问服务器中的相关资源。在创建本地用户账号时，Windows Server 2003 会自动将账号名称和有关的信息存放在本地的安全数据库中，而不会复制到其它的域中。当用本地账号登录网络时，服务器便在本地安全数据库中查询该账号的名称，同时检查对应的密码，只有用户名和密码都符合的账号才可以登录到服务器上。

在 Windows Server 2003 中创建的新账号一般都是本地用户账号，在这个账号中包括了用户的名称、密码、所属的组别和个人信息等信息。创建新账号可以参照下面的步骤来完成：

STEP 1 依次单击“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”。

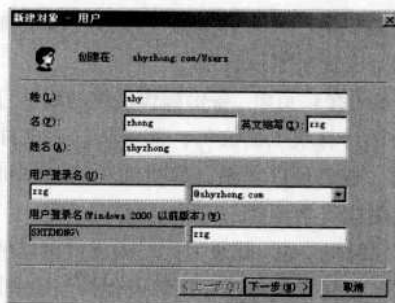
STEP 2 在弹出的对话框中可以看到刚才安装活动目录时设定的域名（此处为“shyzhong.com”），在其中有一个名为“Users”的文件夹，选中之后，可以看见当前 Windows Server 2003 系统中的所有用户名称。使用鼠标右键单击“Users”文件夹，在弹出的菜单中选择“新建”→“用户”。

第五章 组建中小型企业网络



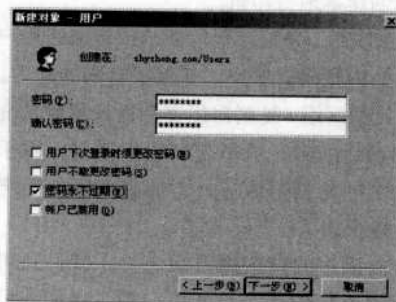
新建用户

STEP 3 根据需要，输入员工的姓、名、英文缩写和用户登录名，然后单击“下一步”按钮。



输入详细信息

STEP 4 需要设置有关员工的密码内容，其一是要在密码输入框中输入两个完全一致的密码，或者是不填写密码，但是不填密码时要选中下部的“用户下次登录时须更改密码”选项。在设置密码的时候要注意位数最好在8位以上，而且需要将大小写的英文字母和数字及特殊符号混合起来使用，这样才能够保证密码的安全性（如“shzhong77”）。

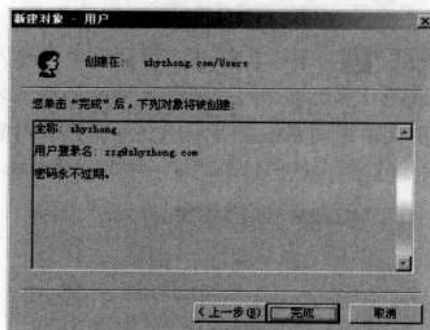


设置复杂的密码

在对话框的下部还有几个关于密码的设置内

容，如“用户下次登录时须更改密码”可以让用户在下次使用该账号登录服务器时，必须先更改密码才可以登录；“用户不能更改密码”可以让用户无法自行更改密码；“密码永不过期”能够让密码长期有效；“账号已停用”则是暂时停用这个账号，使该账号无法正常登录服务器。然后，单击“下一步”按钮继续。

STEP 5 下一步中提供了前面有关用户账号的设置信息，检查无误后，单击“完成”按钮，完成员工账号的创建。



完成账户创建

STEP 6 创建好员工账号之后，再返回到“Active Directory 用户和计算机”对话框，此时可以发现多出了一个用户账号，这就说明员工账号设置已经成功了。



账户列表

STEP 7 创建好用户账号之后，有时还需要对账号进行重新设置密码、修改和重新命名等操作，所以管理用户账号也是一个非常重要的部分。

STEP 8 用户添加完毕后，还需要在域中将客户机添加进来。在“Active Directory 用户和计算机”对话框中，用鼠标右键单击“shzhong”。

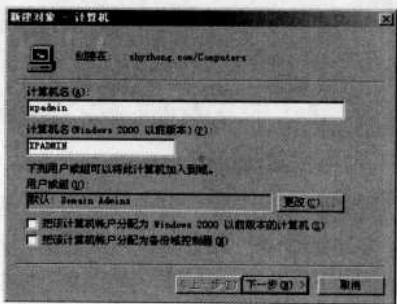


com”域下的“Computers”，在弹出的菜单中依次单击“新建”→“计算机”。



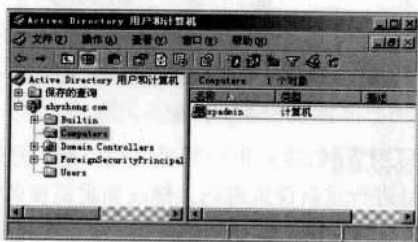
新建计算机

STEP 9 在下一步打开的对话框中，输入要加入域的计算机名即可。要加入域的计算机名最好为英文，否则系统会提示中文计算机名可能会引起一些问题。然后单击“下一步”按钮继续。



输入详细内容

STEP 10 在下面出现的对话框中，只需一路单击“下一步”按钮，即可完成设置。最后，单击“Active Directory 用户和计算机”对话框中的“Computers”，在其右侧对话框中随即可以看到刚刚添加的计算机。



计算机列表

在完成了上述操作后，有兴趣的读者还可以继续学习下面的内容，否则可以跳过：

❖ 100 ❖

在域控制器中有了新用户之后，因为企业局域网中有数以百计的用户，所以，为了简化网络的管理工作，Windows server 2003 中提供了用户组的概念。所谓“用户组”就是指具有相同或者相似特性的用户集合，比如我们可以为某个办公室中的用户创建一个专门用户组，接着，只要给用户组设置了相关的权限，位于这个用户组中的用户就会自动继承这个组的权限，这样可以大大减少设置用户账号的时候的麻烦。

在安装 Windows server 2003 的时候，系统会自动创建内置组，它主要由下面几个部分组成：

> 管理员组：管理员组的成员具有对计算机的完全控制权限，只有内置组才被自动授予该系统中的每个内置权利和能力。

> 备份操作员组：备份操作员组的成员可以备份和还原计算机上的文件，而不管这些文件的权限如何。他们可以登录计算机和关闭计算机，但是不能更改安全设置。

> 超级用户组：超级用户组的成员可以创建用户账号，但是只能修改和删除由他们创建的账户。超级用户组可以创建本地组，并从他们创建的本地组中删除用户，也可以从超级用户、用户和来宾组中删除用户。他们不能修改管理员或备份操作员组，也不能拥有文件的所有权，备份、还原目录，以及加载和卸载设备驱动程序。

> 用户组：用户组的成员可以执行大部分普通任务，比如运行程序、使用本地和网络打印机以及关闭和锁定工作站。用户可以创建本地组，但是只能修改自己创建的本地组，他们不能共享目录或者创建本地打印机。

> 来宾组：来宾组允许偶尔或者临时用户登录工作站的内置来宾账户，并授予有限的能力。

> 复制器组：复制器组支持目录复制功能，而且复制器组的唯一成员是域用户账号，用于登录域控制器的复制器服务，不能将实际的用户账号添加到这个组中。

除去上述的这些内置组之外，我们还可以根据实际需要来创建自己的用户组。比如我们可以将一个部门的用户全部放置到一个用户组中，然后针对这个用户组进行属性设定，这样就能够快

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

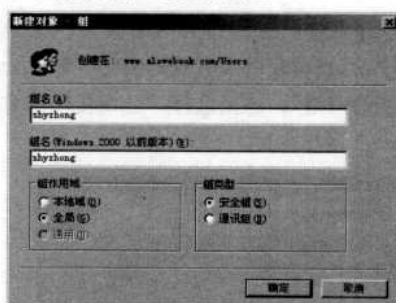
第五章 组建中小型企业网络

速完成组内所有用户的属性改动。具体的用户组创建可以按照下面的步骤来完成。

STEP 1 依次单击“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”。

STEP 2 在打开的窗口中右击“Users”文件夹，在弹出的菜单中选择“新建”、“组”命令。

STEP 3 在弹出的新建组窗口中的“组名”中填写新建用户组的名称，比如 shyzhong 之类的名称，然后它会自动出现在下部的“组名 (Windows 2000 以前版本)”文本框中。



新建用户组

那么这里的“组作用域”选择“本地域”还是“全局”呢？由于办公室组建的局域网只有一个域控制器，所以两者在功能上的差别并不大。但是考虑到今后网络扩展，所以建议用户选择“全局”。至于“组类型”中的两个方式，“安全式”比“分布式”要强大，例如使用“安全式”之后可以设定网络中的访问权限，而“分布式”就没有这个功能，所以在办公室组建的网络中建议采取“安全式”。确定之后即可完成用户组的创建工作。

STEP 4 此时再返回到“Active Directory 用户和计算机”窗口，可以看见右边区域多出了一个用户组的图标。



注意

需要提醒用户注意的是，用户和用户组的图标是有一些差别的：用户的图标只有一个头像标识，而用户组则是由两个头像组成的，所以用户还是很容易区分的。

完成了用户组的创建之后，我们就需要在这

个用户组中添加一些用户。由于属于组的用户具有授予该组的所有权限，因此如果用户是多个用户组的成员，那么这个用户就拥有授予他所属的每个用户组的权限。在用户组中添加新的用户，可以按照下面的方法完成：

STEP 1 在“Active Directory 用户和计算机”窗口中选择“Users”文件夹。

STEP 2 选择需要添加用户的用户组并使用鼠标右键单击用户组图标，在弹出的菜单中选择“属性”。

STEP 3 在出现的属性窗口中，会显示关于这个用户组的相关信息，比如组名、描述和电子邮件等。



用户组相关信息

STEP 4 切换到“成员”选项卡，选择下部的“添加”按钮激活用户选择窗口。在这个窗口中可以看出当前所有的用户。

STEP 5 用鼠标选择需要添加到用户组中的用户名单，单击“添加”按钮将其添加到下部的用户账号列表中。



添加用户组成员

如果有很多用户需要添加的话，还可以通过“Ctrl”按钮来一次性选择多个用户，最后选



择“确定”按钮。返回到“成员”选项卡界面后就可以看见我们选中的用户已经添加到用户组中了。

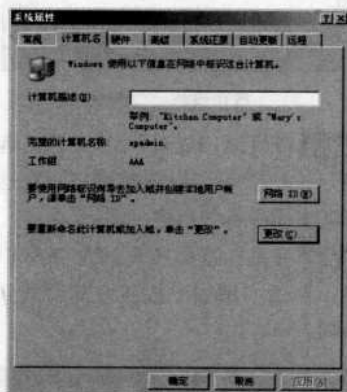


如果遇到部门解散等特殊情况，系统管理员可以将这个用户组删除。不过在删除用户组之后，用户组中的用户并不会被删除，他们仍然存在。删除用户组的时候只要在 Active Directory 用户和计算机窗口中找到需要删除的用户组，然后右击鼠标并在弹出的窗口中选择“删除”命令即可完成。

2. 客户端的设置

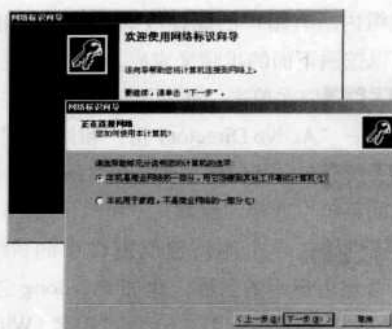
以 Windows XP Professional 作为客户端操作系统为例，加入 Windows Server 2003 域时，应做如下设置：

STEP 1 用鼠标右键单击“我的电脑”图标，在弹出的快捷菜单中选择“属性”。然后，在打开的“系统属性”对话框中切换到“计算机名”标签页，确认计算机名与加入域的计算机名是一致的。



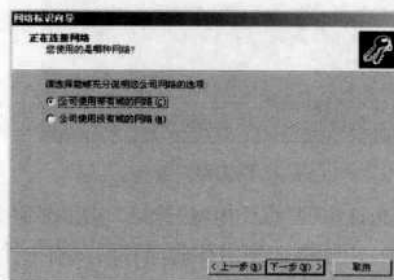
设置计算机名称

STEP 2 单击“网络 ID”按钮，在出现的“网络标识向导”中单击“下一步”按钮进入“选择如何使用本计算机？”界面，然后选择“本机是商业网络的一部分，用它连接到其它工作着的计算机”项并单击“下一步”按钮继续。



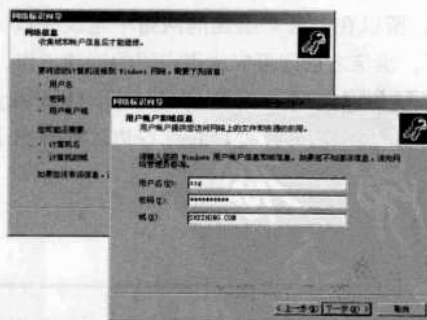
网络标识向导

STEP 3 需要确定使用的网络类型，这里也有两个选项：“公司使用带有域的网络”和“公司使用没有域的网络”。这里选择“公司使用带有域的网络”。



设置网络类型

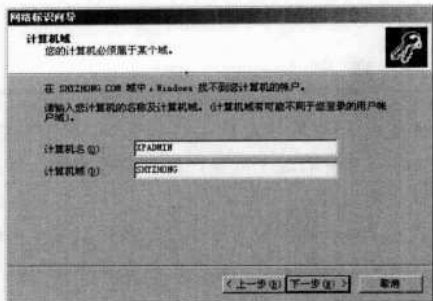
STEP 4 单击“下一步”按钮后，会提示必须获得有关域和账户信息之后才可以操作。接下来输入登录域的用户名、密码和域名。



设置域和账户信息

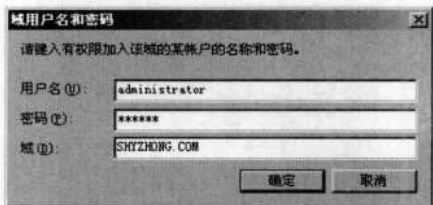
STEP 5 在出现的如图所示界面中，需要输入要登录域的计算机名和相应的域名。

第五章 组建中小型企业网络



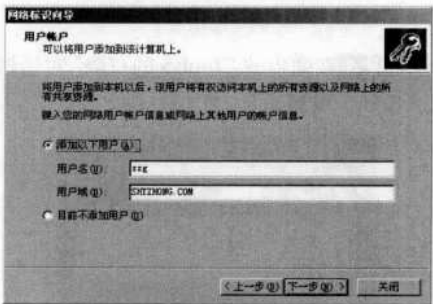
设置域名

STEP 6 需要设置有权加入这个域的用户账号的名称和密码。一般说来，需要用户输入“administrator”作为用户名，并且在密码框中输入已知的系统管理员密码，最后在“域”中输入设定好的域名称（如“shyzhong.com”）。



输入登录账户信息

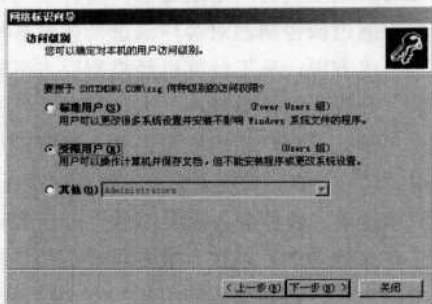
STEP 7 单击“确定”按钮后，如果信息正确，那么将会出现添加用户到本机的对话框。选择默认状态后单击“下一步”按钮继续。



添加用户信息

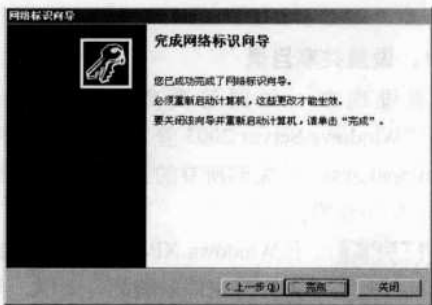
STEP 8 需要设定本机用户的访问权限，这里提供了标准用户、受限用户和其它 3 种类别。其中标准用户可以修改电脑设置并安装程序，但是不可以阅读属于其它用户的文件；受限用户能够操作电脑并保存文件，但是不可以安装程序或

进行可能对系统文件和设置有潜在破坏性的更改。建议用户选择“受限用户”来保障系统的安全。



设置权限

STEP 9 Windows XP 客户端的电脑设置就完成了，单击“完成”按钮后，重新启动电脑。



完成设置

STEP 10 电脑重新启动完毕后，即可以用“zzg”这个账户使 Windows XP 客户机登录 Windows Server 2003 的“SHYZHONG”域。



域环境下的登录

稍后，打开“网上邻居”对话框，从中应该能够看见自己和其它的电脑，这就表示 Windows XP 与 Windows Server 2003 之间的域模式局域网已经组建完成了。



5.3.3 软件分发

在完成域模式的网络组建后，网管就可以在域环境中通过域控制器对客户端进行各种各样的管理了。比方说，员工计算机经常需要进行软件的安装、升级、维护等操作，为了规范软件安装以及避免因此可能产生的安全问题，域管理员可以使用“软件分发”功能来完善地管理这项任务。

简单地说，软件分发就是将软件分布发送到指定工作站的功能。以往，很多管理员都是采用了共享的方法，但共享所能引起的安全隐患往往会成为网管们心中永远的痛！此时，如果你尝试使用软件分发功能的话，那么你将会惊喜地发现企业工作站的软件安装将会变得轻松自如且安全无忧！

1. 设置共享目录

假设现在一位网管要将 shyzhong.com 域中的“Windows Server 2003 管理工具包”程序“Adminpak.msi”分发到所有的工作站上，那么则应进行如下设置：

STEP 1 由于 Windows XP/2003 等系统的安全设计都是基于 NTFS 文件系统的，所以，需要在使用 NTFS 文件系统的分区中新建一个目录，如在 C 盘中新建一个名为“Tools\$”的目录。

STEP 2 将“Adminpak.msi”程序从 Windows Server 2003 安装光盘的“I386 目录”中复制到 C 盘的“tools\$”目录中。

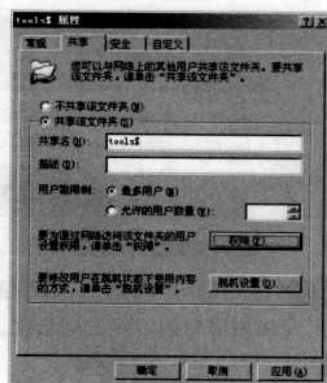


指定文件位置



准备用于共享的目录名，如果带有“\$”符号，则网络中不能看到这个目录，但可以通过输入路径的方法来访问到它；如果不带有“\$”符号，则网络中可以看到它。在软件分发操作中，只有让用户在网络中不能直接看到共享目录，才能把管理和控制权牢牢地把握在网管手中。

STEP 3 在 C 盘中右键单击“Tools\$”目录，在弹出的菜单中选择“共享与安全”。在弹出的“Tools\$ 属性”对话框的“共享”选项卡设置界面中，勾选“共享该文件夹”项后，单击下方的“权限”按钮。



共享选项卡

STEP 4 在弹出的“Tools\$ 的权限”对话框中，单击“添加”按钮。

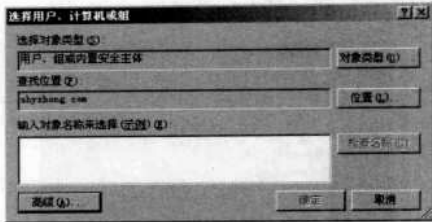


单击添加按钮

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第五章 组建中小型企业网络

STEP 5 在“选择用户、计算机或组”窗口中单击“高级”按钮。



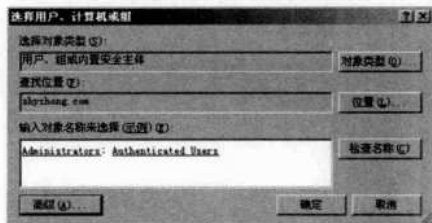
单击高级按钮

STEP 6 在随之切换的窗口中单击“立即查找”按钮，将当前系统中的用户、计算机等资源查找出来，在按住 Ctrl 键的同时，使用鼠标单击选择其中的“Administrator”组和“Authenticated Users”组后，单击“确定”按钮。



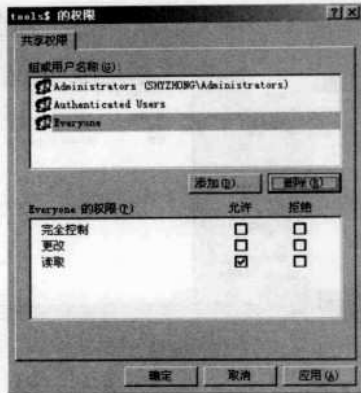
选择账户

STEP 7 在返回到标准模式的“选择用户、计算机或组”窗口后，可以看到选中的两个组均已添加，此时请单击“确定”按钮。



返回列表窗口

STEP 8 在返回到“Tools\$ 的权限”对话框后，选中“Everyone”项后单击“删除”按钮将其删除。



删除Everyone

STEP 9 分别选中“Authenticated Users”组，将其共享权限设置为“读取”、选中“Administrators”组后，将其权限设置为“完全控制”。



设置权限

注意

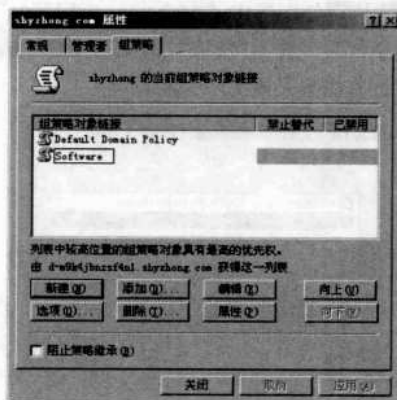
分发的软件必须是 MSI 封装文件，如果想将非 MSI 格式的文件封装成 MSI 文件，可以使用 InstallShield 等工具来完成这个转换操作。当然，也可以使用 ZAP 文件来分发非 MSI 格式的文件。

STEP 10 在以域管理员身份登录 DC（即域控制器），依次单击“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”菜单。在弹出的窗口右键单击“shyzhong.com”，在弹出的菜单中选择“属性”。



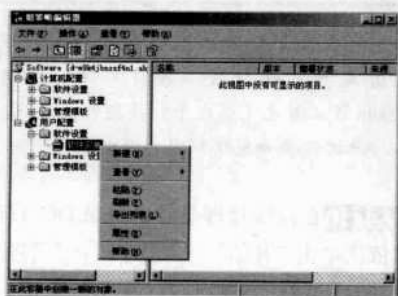
选择属性

STEP11 在打开的“属性”窗口中单击“新建”按钮，并将新建的组策略对象命名为“Software”。



命名策略

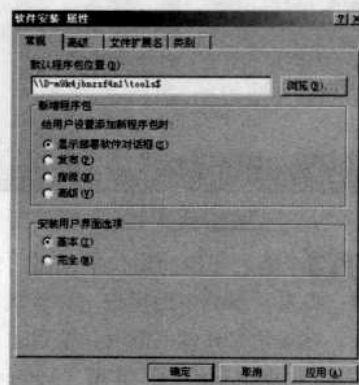
STEP12 选中 Software 并单击下方的“编辑”按钮，在打开的“组策略编辑器”窗口中依次单击“用户配置”→“软件设置”→“软件安装”项，右键单击“软件安装”项，并在弹出的菜单中选择“属性”。



选择属性

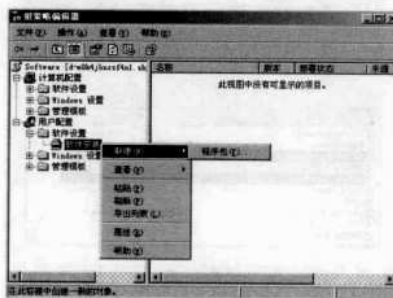
STEP13 在弹出的“软件安装 属性”对话框

中手工输入“\\计算机名\共享文件名”（如“\\D-m9k4jbnzsf4n1\tools\$”），单击选中“显示部署软件对话框”和“基本”两项。



输入路径

STEP14 单击“确定”按钮返回后，右键选中并单击“软件安装”项，在弹出的菜单中依次选择“新建”→“程序包”项。



新建程序包

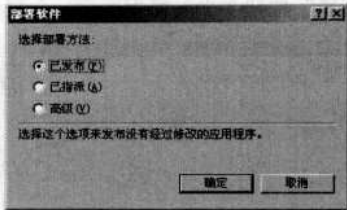
STEP15 在随后弹出的“打开”对话框中，选中 tools\$ 目录下的“Adminpak.msi”文件后，单击“打开”按钮。



选择安装文件

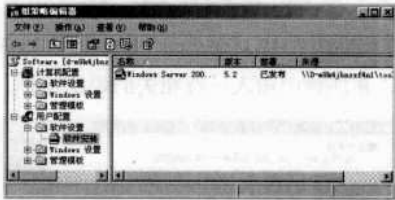
第五章 组建中小型企业网络

STEP16 在随后弹出的对话框中选中“已发布”项并单击“确定”按钮，稍后关闭组策略对话框。



选择已发布

STEP17 在组策略窗口的“软件安装”项右侧窗口可以看见刚刚加入的程序包。



添加的程序包

STEP18 依次单击“开始”→“程序”→“附件”→“命令提示符”菜单项，输入“Gpupdate”命令并回车，刷新组策略后即可使设置立即生效。

2. 在工作站中安装软件

经过上述的设置后，软件就会被分发到隶属于 shyzhong.com 域的所有客户机上了。在客户机（以 Windows XP 为例）登录到域后，只需单击“添加/删除程序”窗口中的“添加新程序”按钮，就会立即在“从网络添加程序”列表中列出 DC 中分发的“Adminpak.msi”程序了。



安装项目

此时，只需单击“添加”按钮即可立即进行程序的安装了，安装的过程和本机安装没什么区别。

别，只不过速度稍微有点慢罢了。

5.3.4 高效管理企业资源

组建企业网络的优点之一，就在于能够通过网络高效地管理所有计算机里的资源。通常，在企业很多计算机中都会有共享资源，要想访问这些资源的话，就需要每台计算机的名称以及共享资源的名称。那么，能不能让员工只记住一个固定的名称来使用这些不同的共享呢？Windows Server 2003 中提供的 DFS 就可以解决这个问题。

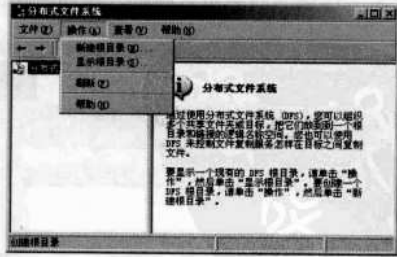
1. 资源管理实战

分布式文件系统 (DFS) 是一个单层文件系统，DFS 提供文件系统资源的逻辑树结构，该资源可能处于企业网络的任何地方。由于 DFS 树是单点索引，所以企业网中的用户可以访问基于数据含义表达的网络资源，而不必考虑基本资源的确切位置，也无须知道和指定网络分配文件的确切物理位置。

执行如下操作，可以在企业网络中使用 DFS 技术管理所有的共享资源：

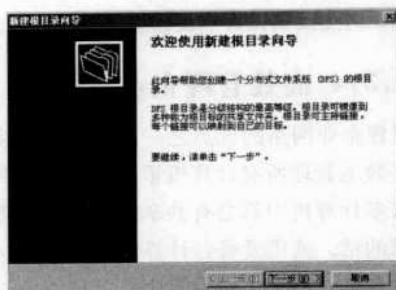
STEP1 在服务器中以管理员身份登录，在 C 盘分区的根目录下创建一个名为“DFS_SHARE”的文件夹（即 C:\DFS_SHARE），并设置此目录为共享。

STEP2 在“管理工具”中运行“分布式文件系统”，在打开的窗口中依次单击“操作”→“新建根目录”菜单。



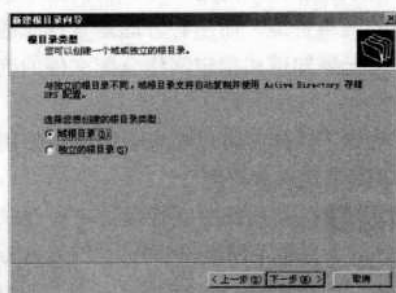
分布式文件系统管理界面

STEP3 在弹出的“新建根目录向导”运行界面中，依次单击“下一步”按钮继续。



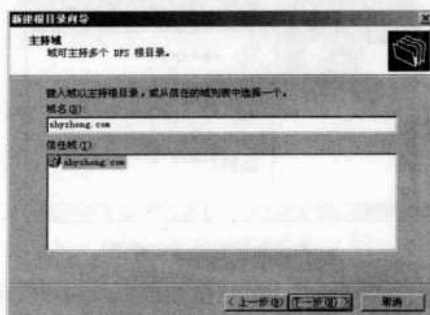
根目录向导

STEP 4 出现如图所示的界面时，选择“域根目录”项继续，因为 Windows Server 2003 服务器通常都会配置活动目录，因此选中此项可以启用活动目录存储 DFS 树状拓扑结构，同时也可以使分布式文件系统支持 DNS 命名和文件副本复制的特性。



设置根目录类型

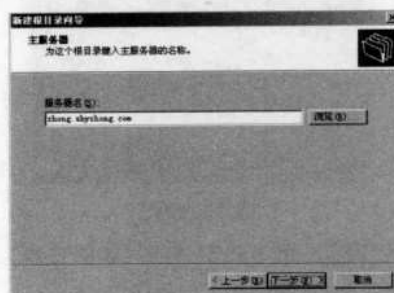
STEP 5 在“主持域”界面中向导会将当前计算机所在域作为首选项，并将该域的域名和域的图标分别显示在“域名”列表框和“信任域”列表框中，这里建议使用系统默认域选项继续。



设置主持域

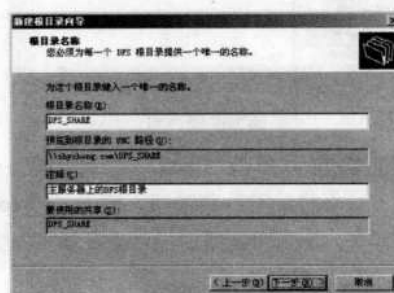
STEP 6 切换后出现如图所示的“为这个根

目录键入主服务器的名称”界面，在“服务器名”中输入当前计算机在域中的名称。此外，也可以单击“浏览”按钮在当前域中选一台服务器。



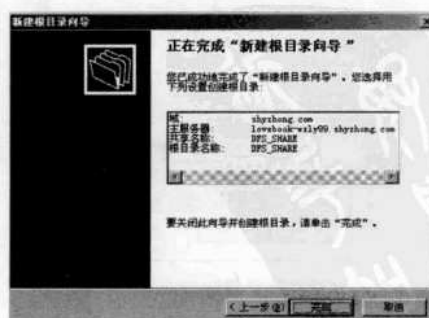
设置主服务器

STEP 7 在“根目录名称”栏中输入“DFS_SHARE”，在注释中输入一些相关的说明信息。



输入说明信息

STEP 8 当出现界面时，需要指定“DFS_SHARE”目录的路径。在最后出现的如图所示界面中，向导将会把新建的 DFS 根目录的所有信息都显示在对应的文本框中，此时只需单击“完成”按钮即可结束安装分布式文件系统的所有操作。



完成设置

STEP 9 在返回到“分布式文件系统”控制

第五章 组建中小型企业网络

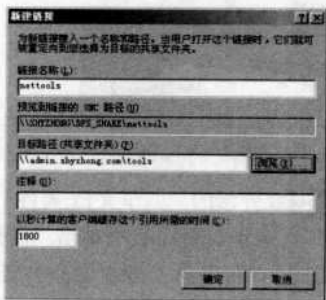
台窗口中,可以看到新建的 DFS 根目录显示在“分布式文件系统”列表框中。



“分布式文件系统”列表框

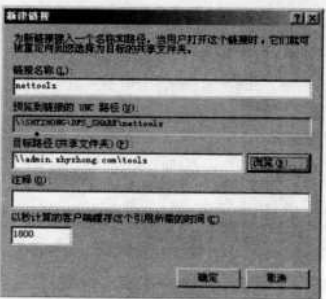
创建 DFS 根目录后,接着需要把其它计算机上提供的共享资源添加到 DFS 根目录中,才能体现出 DFS 的强大功能。为此,需要执行如下操作:

STEP 1 在如图所示的“分布式文件系统”窗口中,右键选中并单击已创建好的 DFS 根目录,在出现的菜单中选择“新建 DFS 链接”。



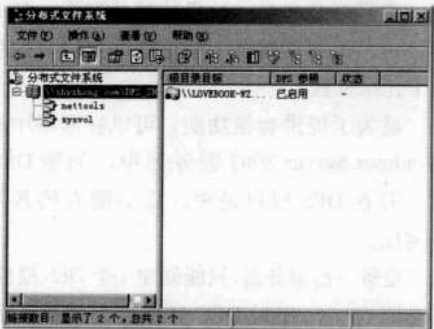
新建DFS链接

STEP 2 在弹出的“新建链接”对话框中,在“链接名称”项中为共享链接创建一个名称。单击“浏览”按钮,指定此共享链接的具体路径。



选择共享资源

STEP 3 设置完毕并单击“确定”按钮完成 DFS 链接的创建后,重复这几个步骤将企业网络中的所有共享资源在 DFS 根目录中创建 DFS 链接。添加完 DFS 链接后,在返回到“分布式文件系统”窗口后,可以看到添加的共享资源链接。



DFS链接

完成上述的 DFS 应用,企业网络中的计算机该怎么使用这项功能呢?方法非常简单,Windows 用户均可以通过打开“网上邻居”窗口,在这里依次双击打开提供 DFS 服务的服务器→DFS 根目录名,就可以看到所有已添加的、位于不同计算机中的共享资源了。



访问共享资源

网络管理员可以定期更新 DFS 根目录中的共享,也可以随时将一些共享添加到 DFS 根目录中供大家使用。

3. 几个问题

在使用分布式文件系统 (DFS) 时,还应该注意以下几个问题:



一是为了避免打开“网上邻居”时，一下浏览到许多共享（这些共享已经通过 DFS 链接方式添加到 DFS 根目录中）而无从分辨哪个是 DFS 根目录，可以在创建这些普通的共享时，使用隐含的共享（共享名后加一个 \$ 符号）。这样，网管可以统一掌握这些共享，并将这些共享添加到 DFS 根目录中，用户不需要了解这些共享以及这些共享处于什么位置。

二是为了提供容错功能，可以在网络中的多台 Windows Server 2003 服务器中，创建 DFS 根目录，并在 DFS 根目录中，添加所有的共享为 DFS 链接。

三是每一台服务器，只能创建一个 DFS 根目录。

总而言之，使用 DFS 可以极大地减少网络管理员的负担，减轻用户记忆许多共享目录的困难，而且相关的操作又比较简单，推荐大家在基于 Windows 2000/2003 系统的企业网络中使用。

5.4 企业环境中的共享应用

局域网最大的魅力就在于共享，根据需要可以对文件、打印机、刻录机、磁盘、光驱等设备进行网络共享。这样就极大地扩展了网络的功能，以及有效提高了软件和硬件资源的使用率。

5.4.1 文件共享

所谓“文件”共享，是指将自己计算机中的文件提供给网络中的其它计算机访问、复制、新建或是删除。通过在网络中共享文件，可以省却以往文件使用磁盘复制的麻烦。下面，以客户端计算机安装的 Windows XP/Vista 系统环境为例，讲解一下将文件进行共享的过程。在 Windows XP/2003/Vista 中，对文件共享有着诸多的权限管理，这些能有效地保证共享资源的安全。

1. Windows XP中共享文件

在 Windows XP 中共享文件可以有两种方法，一种是使用“共享文档”这个目录；另一种是手工创建共享资源。

(1) 使用“共享文档”

默认状态下，Windows XP 将会自动创建一个

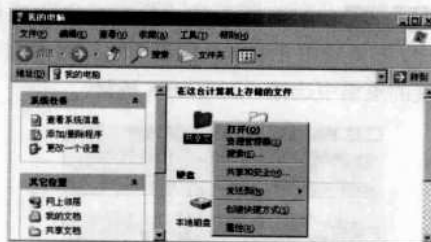
名为“共享文档”的共享目录。



共享文档

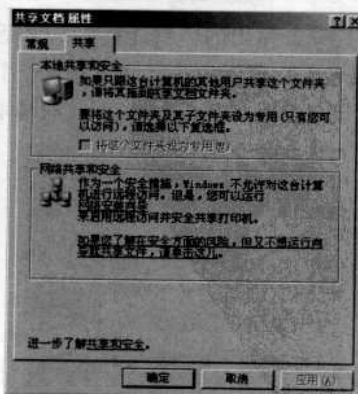
用户只需稍加设置，就可以利用这个现成的共享目录，很轻松地实现局域网间的文件共享了。为此，需要执行如下操作：

STEP 1 右键选中“共享文档”目录并单击，在弹出的菜单中选择“共享与安全”项。



选择“共享与安全”

STEP 2 在弹出的“共享文档 属性”窗口中，在“共享”选项卡设置面板中单击“网络共享与安全”部分的“如果您了解在安全方面的风险，但又不想运行向导就共享文件，请单击这儿”。



设置共享

第五章 组建中小型企业网络

STEP 3 在弹出的“启用文件共享”对话框中，选中“只启用文件共享”项后单击“确定”按钮关闭对话框。

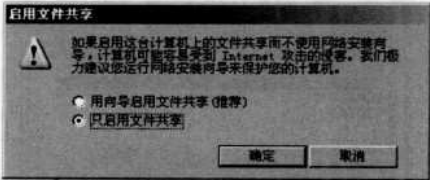


图 5-1-1 启用文件共享对话框

STEP 4 随即在“共享文档 属性”窗口中切换到“共享”选项卡，这里的“网络共享与安全”部分将呈现可设置状态。此时，勾选“在网络上共享这个文件夹”项和“允许网络用户更改我的文件”项后，单击“确定”按钮关闭属性对话框。

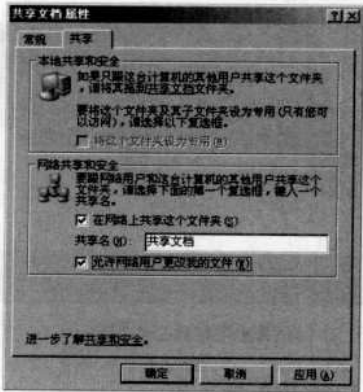


图 5-1-2 共享文档 属性对话框

STEP 5 “允许网络用户更改我的文件”项的选中，表示局域网中的其它用户可以对这个目录进行“写”操作。在上述设置完毕后，局域网上的其它计算机就可以通过“网上邻居”访问到“共享文档”及其中的资源了。

(2) 手工创建共享资源

除了可以使用“共享文档”进行文件的共享外，也可以在 Windows XP 手工创建共享资源。创建模式有两种，即“简单共享”和“非简单共享”两种模式，以后者为例，需要执行如下操作：

STEP 1 依次单击“开始”→“设置”→“控制面板”→“文件夹选项”，在打开如图所示的对话框后，在“查看”选项卡列表中清空“使用简

单文件共享（推荐）”项的勾号。

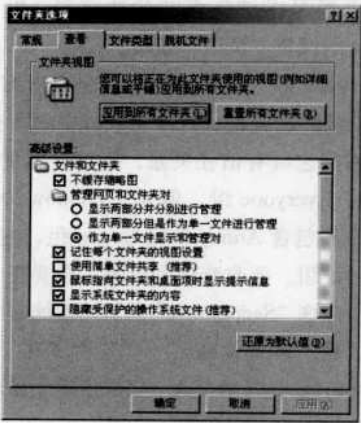


图 5-1-3 文件夹选项对话框

使用针对初级用户设计的“简单共享”功能，可以让用户设置共享资源时非常容易。但是，却有三个限制，即：

- * 无法进一步对共享资源进行各种定制。
- * 不允许设置 NTFS 访问权限，即不能出现“安全”选项卡。
- * 简单共享方式默认使用 Guest 账户登录。

STEP 2 在取消“简单共享”的勾选状态后，右键单击要设置为共享的资源，在弹出的菜单中选择“共享和安全”。在打开属性窗口后，就可以看到共享界面和“安全”选项卡了。

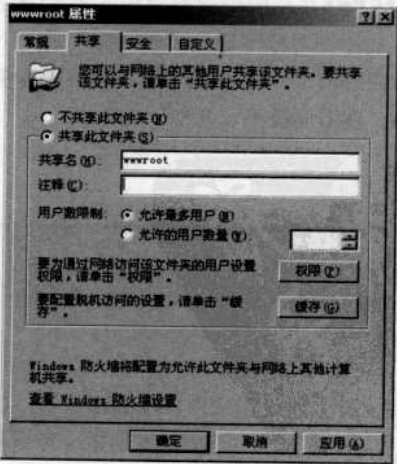
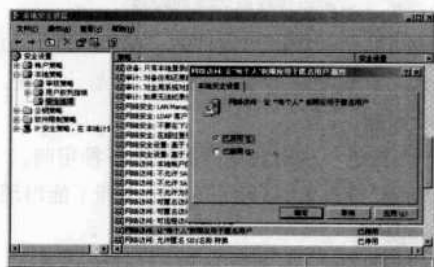


图 5-1-4 共享选项卡



STEP 3 在勾选“共享此文件夹”项后，虽然这样已经可以进行资源的共享了，默认会对 Everyone 组设置“读取”权限。

Everyone 即“每个人”组，包含所有能够访问当前电脑的账户，包括 Guest 和域中的所有账户。如果域和其它域有信任关系，则信任域的所有账户都属于 Everyone 组。但是，Windows XP 中的这个组中不包含 Anonymous Logon 组，也就是不包含未认证组。要改变这个范围，需要在“运行”栏中使用命令“Secpol.msc”打开“本地安全策略”窗口后，将“本地策略”→“安全选项”节点下的“网络访问：让‘每个人’权限应用于匿名用户”项的状态设置为“已启用”即可。



启用策略

在早期的 Windows 版本中，Everyone 组的设计一直是个很大的安全隐患，因为 Everyone 的权限设置不当导致的入侵例子数不胜数。

STEP 4 在权限设置窗口中，需要遵循“最小化”的原则对权限进行设置，而不是一下子将最高权限放出来。比方说，“读取”权限能满足需求的话，就不要授予“更改”权限。



强烈建议不要对“Documents and Settings”、“Windows”等系统文件夹，以及不能被其它用户进行配置的文件夹。

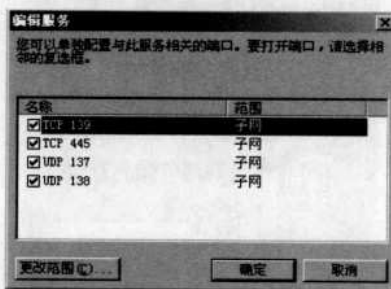
在执行上述设置文件共享的操作后，还需要在 Windows 防火墙中开放共享通道，否则共享的资源是无法被网络中的其它计算机访问的。也就是说，需要在“Windows 防火墙”中设置“文件

和打印机共享”项为勾选状态。



开放共享通道

这样才能开放共享资源的访问端口 137、138、139（传统的 NetBT）和 445（TCP/IP 上的 SMB 直接承载）。



共享功能使用的端口

2. Vista 中共享文件

在 Vista 中可以通过如下几种不同方式，将自己的文件或文件夹在网络中进行共享。

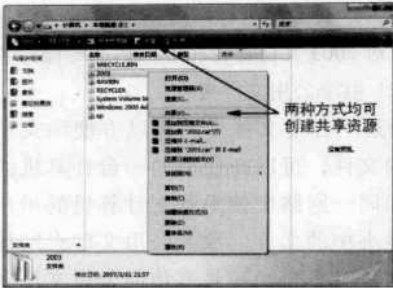
（1）共享任何文件夹

用户可以对计算机中的任何文件夹进行共享，这是 Vista 中设置共享的一种方法。这种共享设置方法，可以决定哪些人可以更改共享文件，以及可以做什么类型的更改（如果有），可以通过设置共享权限进行相应的管理。

以将 E 盘分区下的“2003”文件夹进行共享为例，需要执行如下操作：

STEP 1 在“计算机”窗口中进入“E”分区窗口。此时，在单击选中“2003”文件夹后，既可以单击工具栏中的“共享”按钮，也可以单击右键并在弹出的菜单中选择“共享”项。

第五章 组建中小型企业网络



创建共享的方法

STEP 2 使用上述两种方式均可以进入“共享向导”对话框。

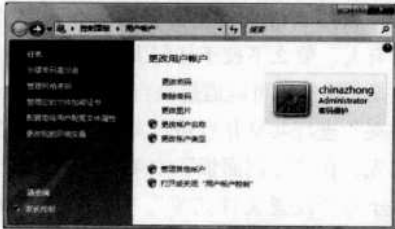
STEP 3 在“文件共享”对话框中，既可以授权默认选用的账户来访问本机的共享资源，也可以执行如下的使用其它账户的操作：

- * 键入事先创建的有权限共享此资源的账户名称，并单击“添加”按钮。
- * 单击用户名文本框右边的箭头，在弹出的下拉列表选择一个账户名称，并单击“添加”。



添加账户

* 如果列表中看不到有权限共享资源账户名，那么可以单击用户名文本框右边的箭头，在弹出的下拉列表中单击“创建新用户”。在自动弹出的如图所示窗口中单击“管理其它账户”项。

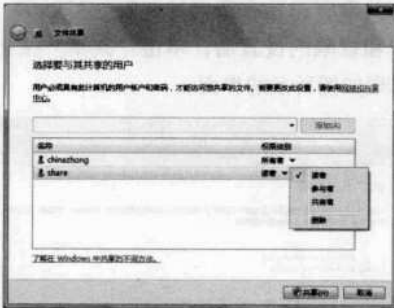


管理账户

STEP 4 在弹出的窗口中，单击“创建一个新账户”链接并根据提示完成专门供其它计算机用户用来访问本机共享资源的账户（推荐为标准账户级别）。

在完成新账户的创建后，再次打开共享窗口，即可在用户名列表中找到刚创建的账户了。此时，单击“添加”按钮即可使用此账户。

STEP 5 在完成了账户的选择后，在如图所示的窗口中单击每个账户右侧“权限级别”列中的下向箭头，在弹出的下拉菜单中可以看到多个共享权限级别。



选择共享级别

其中，各个权限级别对应的操作范围是：

- * 读者：限制用户或组只能查看共享文件夹中的文件。
- * 参与者：允许用户或组查看所有文件、添加文件，以及更改或删除他们所添加的文件。
- * 共有者：允许用户或组查看、更改、添加和删除共享文件夹中的文件。



注意

如果共享的是文件而不是文件夹，则没有将权限级别设为“参与者”的选项。

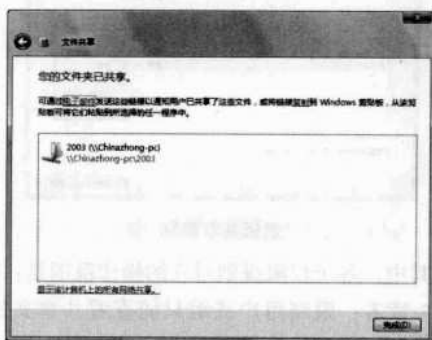
除了上述三项外，要注意“删除”项并不代表共享权限。它的作用仅是在列表中删除左侧对应的账户名。通常，我们可以根据需要进行一个账户、多个账户或一组账户设置共享权限。举个例子：现在想将 2003 文件夹共享，并授权 A 同事使用 001 这个账户访问此文件夹。此外，又



想授权 B 同事使用 002 这个账户具有管理文件夹的权限，那么我们就可以这样来完成这样任务：

首先创建 001 和 002 两个账户，并在 2003 文件夹的“文件共享”对话框中添加这两个账户。接着在“权限级别”列表中，为 001 账户勾选“读者”权限，为 002 账户勾选“参与者”或“共有者”权限即可。完成设置后，同事 A 和 B 就可以使用具有不同权限的专用账户对 2003 进行共享访问了。

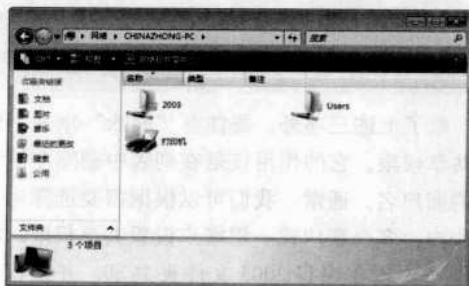
STEP 6 通常，如果没有特殊的共享应用需求的话，只需设置当前账户（即默认选用的账户）对所有共享资源具有所需的权限就可以了。在完成账户和权限的设置后，单击“共享”按钮后即将出现如图所示的界面。



完成共享

STEP 7 此时，可以看到 2003 这个文件夹已经共享成功。所以，现在单击“完成”按钮即可结束共享任务了。

现在，就可以在局域网中的任一计算机的“网络”窗口中双击当前计算机的图标，在完成登录操作后就可以看到共享的 2003 文件夹图标了。



访问共享资源

此时，双击此图标即可使用当前账户拥有的权限，对 2003 文件进行相应的访问等操作了。

(2) 共享公用文件夹

通过“公用文件夹”可以方便地共享计算机中的文件，可以与使用同一台计算机的其它用户和同一网络中使用其它计算机的用户共享此文件夹中的文件。放入公用文件夹的任何文件或文件夹将自动被具有访问公用文件夹权限的用户共享。

Vista 中只有一个公用文件夹，即“C:\Users\Public”。本机中具有账户的用户都可以自动共享（不同网络环境中的共享，而是本机中的资源共享。）此文件夹。要打开公用文件夹，可以通过执行如下操作来完成：

STEP 1 打开“计算机”窗口，单击左侧导航窗格中“收藏夹链接”→“公用”。



公用文件夹

STEP 2 打开“计算机”窗口，单击左侧导航窗格中“收藏夹链接”→“公用”。

本机中 Vista 允许具有账户和密码的所有用户都可以访问公用文件夹。在网络环境中，可以由管理员决定是否允许网络中的任何人访问公用文件夹。但是，管理员无法选择哪些账户可以通过网络访问公用文件夹：要么将访问权限授予网络中的所有人，要么不授予任何人。

但是，管理员可以通过执行如下操作，对“公用文件夹”进行共享并且进行共享权限的设置：

首先，在“控制面板”中单击“网络和 Internet”部分的“设置文件共享”项，打开“网络和共享中心”。接着，单击“公用文件夹共享”右侧

第五章 组建中小型企业网络

的下向箭头按钮，展开如图所示的设置选项。



设置选项

这里有三个选项可供设置，第一个选项实际上就是赋予了网络用户拥有“只读”权限；第二个选项是赋予了网络用户拥有“修改”权限；而第三个选项则是关闭了共享：

- * 启用共享，以便能够访问网络的任何人都可以打开文件。
- * 启用共享，以便能够访问网络的任何人都可以打开、更改和创建文件。
- * 禁用共享（登录到此计算机上的用户仍可以访问该文件夹）。

STEP 3 无论是选择第一项还是第二项，网络用户都必须使用带有密码的账户方可访问本机中公用文件夹里的共享资料，除非授权 Guest 账户可以通过网络访问本机。

局域网其它计算机在“网络”窗口访问时，公用文件夹的共享名称将会是“Public”，而不是想象中的“公用文件夹”，这一点需要注意了。

启用公用文件夹的共享后，除了立即共享公用文件夹中自带的资源，还可以把要共享的其它资源复制到公用文件夹，亦可自动实现资源共享。

(3) 高级共享

在设置计算机中除了公用文件夹外的资源时，除了使用共享向导的方法外，还可以使用高级共享来完成资源共享的创建任务。

要使用高级共享有两种方法，一是右键单击

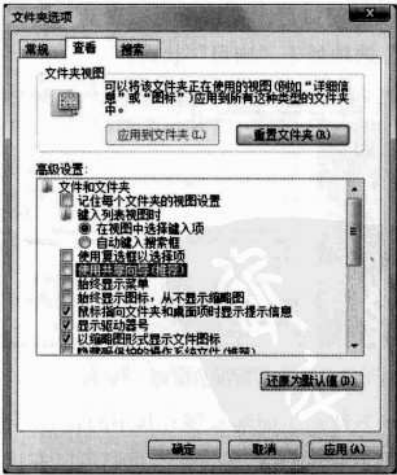
要进行共享的资源，并在弹出的菜单中选择“属性”，在出现的属性窗口中单击切换到如图所示的“共享”选项卡即可。



共享选项卡

二是关闭共享向导后，通过窗口工具栏中的“共享”按钮或资源右键菜单中的“共享”项，均可以直接打开属性窗格中的高级共享界面。如果要关闭共享向导，只需执行如下操作即可：

STEP 1 在“控制面板”中单击“外观和个性化”部分的“文件夹选项”，打开如下窗口。



文件夹选项

STEP 2 清空“使用共享向导（推荐）”项的选中状态，并单击“确定”按钮后，即可关闭共



享向导功能。关闭共享向导后，高级共享界面中“网络文件和文件夹共享”部分的“共享”按钮将呈不可设置状态，这是因为该按钮已经无法成功调用共享向导了。



已经禁用了共享向导

STEP 3 高级共享界面中可以看到下方有一个“密码保护”部分，其中的信息告诉我们：用户必须具有此计算机的用户账户和密码，才能访问共享文件夹。这实际上是 Vista 中一项默认启用的共享设置，在单击“网络和共享中心”项进入如图所示的窗口后，在这里可以看到“密码保护的共享”选项处于“启用”状态。



密码保护功能

单击右侧的下箭头展开其中的设置界面后，可以看到此项的说明等信息。我们可以在这里对此选项进行启用与关闭的设置。

STEP 4 单击“高级共享”按钮后，将会打开如图所示的界面。这里的设置必须在勾选“共享此文件夹”项后方可进行。



高级共享

其中，各个选项的作用如下：

* 共享名：默认状态下会将当前文件夹的名称设置为共享名。在单击“添加”按钮后，可以为当前资源创建新的共享名。

也就是说，一个共享资源可以有多个共享名。我们可以通过为不同的共享名设置不同的访问账户与权限，来完成一个资源多种访问方式的设置。比方说，有三类用户会访问某个资源，那么就可以创建三个共享名，并为其赋予不同的权限，这样三类用户对资源的访问将会得到严格的控制。



权限设置类型

* 权限：单击此按钮将会打开下面的对话框。



权限设置

* 将同时共享的用户数量限制为：默认值为 10 个，意味着同一时间一台计算机只能有 10 个

第五章 组建中小型企业网络

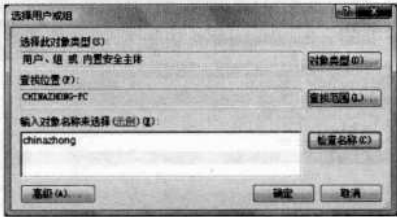
用户共享资源访问。这样的设计主要是为了保护计算机性能不因大量的网络数据传输而产生负荷。

* 注释：在这里可以为每个共享添加注释，这样可以方便以后的权限更改等操作。

这里既可以为默认选用的账户“Everyone”（意思是每一个人，每一个用户）设置共享权限，也可以单击“添加”按钮，添加一个新账户并为其设置新的共享权限。以当前登录的账户设置共享权限为例，执行如下操作：

STEP 1 单击“开始”按钮，并在弹出的菜单右侧窗格顶部可以看到当前登录的账户名，如Chinazhong。

STEP 2 单击“添加”按钮，在弹出的“选择用户或组”对话框中，在“输入对象名称来选择”列表中输入Chinazhong这个账户名。



输入账户名

如果是添加其它账户，则需单击“高级”按钮并在扩展的界面中单击“立即查找”按钮，在搜索结果列表中找到所需的账户并添加即可。

STEP 3 在单击“确定”按钮返回上一步后，选中刚添加的账户并在下方的权限列表中为其设置合适的权限即可。



设置权限

STEP 4 在完成权限的设置后，连续单击“确定”按钮关闭对话框并应用设置即可。

5.4.2 共享打印机

现代办公的空间大多比较紧张，不允许每台计算机旁边都放置一台打印机。通过在网络中共享打印机，可以使用最小的支出获取更多的回报。在共享打印机之前，要明白什么打印机有两种。一种是普通打印机，这种打印机需要连接到计算机中。在计算机中设置此打印机共享后，在计算机处于开机的状态下，别的计算机才能使用它。另一种是网络打印机，这种打印机本身就带有一个网卡，只要将RJ45接口的网线连接到打印机的网卡上就可以实现网络打印。

对于大型企业来说，网络打印机在性能、IP地址设置、操作、配置方面都有着极为出色的表现，不过网络打印机的价格比较昂贵，所以很多企业都是在服务器中安装普通打印机对整个网络共享。

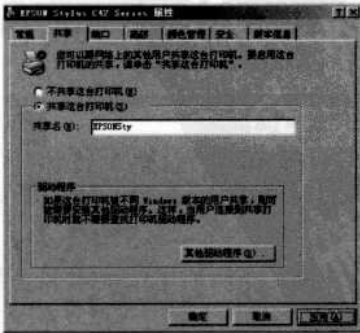
1. 在服务器中共享打印机

以共享Epson（爱普生）STYLUS C42打印机为例，在Windows Server 2003中将该打印机设置为共享状态的方法是：

STEP 1 依次单击“开始”→“设置”→“打印机和传真”菜单。

STEP 2 在打开的“打印机和传真”窗口中，右键选中并单击打算用于共享的打印机图标，在弹出的菜单中选择“共享”项。

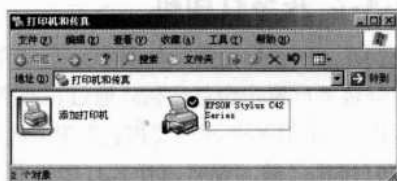
STEP 3 在出现的“共享”选项卡设置界面中，单击选中“共享这台打印机”项并单击“确定”按钮。



共享打印机



STEP 4 在“打印机和传真”窗口中，可以看到 EPSON STYLUS C42 打印机图标下方已经出现了一个手形。这表示该打印机已经呈共享状态。



成功共享

2. 在客户端中使用打印机

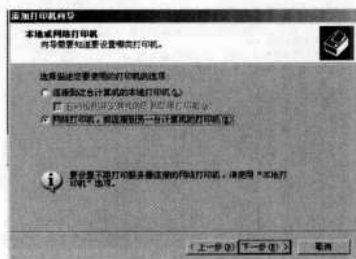
由于大多数的客户端都是 Windows XP，所以，下面讲解如何在这类系统中对服务器里共享的打印机进行安装和使用，需要执行如下操作：

STEP 1 依次单击“开始”→“设置”→“打印机和传真”菜单，打开“打印机和传真”窗口，单击左侧“打印机任务”栏任务列表中的“添加打印机”项。



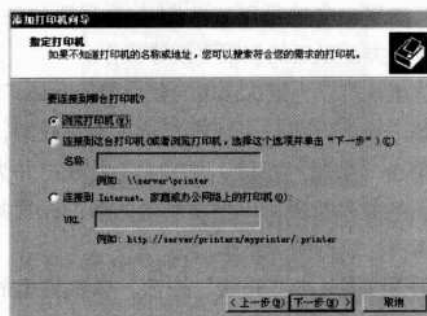
添加打印机

STEP 2 在打开的“添加打印机”向导中单击“下一步”按钮，在“本地或网络打印机”界面中选中“网络打印机，或连接到另一台计算机的打印机”项后继续。



选择网络打印机

STEP 3 在“指定打印机”设置界面中选中“浏览打印机”项后继续。



浏览打印机

STEP 4 在“浏览打印机”对话框中，选中共享打印机 EPSON STYLUS C42 并单击“下一步”按钮继续。



选择打印机

STEP 5 在“默认打印机”设置界面中选择默认状态后，在下一步出现的界面中单击“完成”按钮即可结束共享打印机的设置了。



共享完成

在设置完毕后，就可以在 Word 等支持打印操作的程序中，使用共享的打印机了。

第六章 组建校园网

在计算机硬件价格大幅下降的今天，越来越多的学校打算或已经实现了网络化教学环境。特别是一些已经在每个办公室都配备了计算机的学校，更是迫切希望能够在原有设备的基础上组建起校园网，以期能让所有计算机和设备发挥更大的作用。

校园网的建设是学校向信息化发展的必然选择，校园网是一个功能比较丰富的系统，它不仅为现代化教学、综合信息管理和办公自动化等一系列应用，提供了基本的操作平台，而且能提供多种服务，使信息能够及时、准确地传送给各个角落。

在本章中，将以实例的方式讲解如何实现一个学校的网络化建设。此外，通过学习本章的内容，学校的网络管理员还可以学会如何实现网络教室的创建以及实现 VPN。

6.1 校园网的功能和实施原则

随着教育信息化的发展，网络技术在教育领域得到了广泛的应用，很多学校都组建了校园网，并通过网络的资源共享，使学校体验到了信息化教学所带来的便捷。简而言之，所谓“校园网”就是将校园内各种不同的信息资源通过高性能的网络设备相互连接起来，形成校园内部的 Intranet 系统，对外则通过路由设备接入因特网。

6.1.1 校园网的功能

组建校园网时需要从学校实际情况出发，最大程度地采用可靠的、符合发展趋势的新技术，缜密、周详地对整个校园网络进行规划。准确把握校园网要实现的功能、明确校园网建设的内容。一般来说，校园网与其它网络的不同之处有：

> 为教师和学校领导办公室提供网络，满足教育工作者的办公需要。作为辅助教学的工具，

它可以为学校的教学改革、推行素质教育等方面提供强有力的环境。此外，还可以为教师提供与外校老师交流、学习的途径，共享教育资源。

> 学生机房一般拥有 50~200 台计算机，满足学生的信息技术学习和实践需求。现在计算机和网络技术掌握的程度，已经成为学生步入职场时需要展现的部分能力之一。

> 学生机房的教师机具有管理学生机的能力，满足机房管理的需求。

> 具有独立的服务器机房，满足对内外提供各项服务的需求。比方说，内部网站上可以公布教务信息管理，如课程安排、任课教师安排等等。

> 连接因特网，让学校了解世界，让世界了解学校。

> 学校的数据管理，如教师和学生的档案等等。

> 具有电子图书馆系统，满足对内的图书浏览需求。



很明显，校园网不是一个单纯的办公型网络。它是一个同时具有办公、教学、服务器等一系列应用的复杂型网络。

6.1.2 校园网实施原则

搞好教育就是为国家开创美好的未来，组建校园网不是一个面子工程，而是把信息技术用来提升教育质量，改善教学环境，加深学生对信息理解理解的战略性工程。因此，校园网的实施需要遵守一些原则：

> 新设备选购上：学校用于组建网络的经费大多比较紧张，因此，在设备的选用上要坚持中央节点、服务器、教师与学生机、传输介质等方面都要追求高性价比的产品。不能在一些关键设备上追求高端产品，一些辅助设备上就选用低劣产品，否则校园网络的后期运行就会留下诸多弊端。

> 应用软件上：学校的多媒体机房通常会购买专门的管理软件。在软件的购买上不可贪图便宜选择一些入门级产品，让教师的教学工作产生被动性。而应充分考虑实用性、操作的方便性以及服务保障等因素，让教师能够不断地通过对软件的探索，提高网络化、多媒体化的教学质量。

> 操作系统上：在学校的操作系统选用上，应采用宽松的环境。因为学校充满了学习的氛围，所以，必须让师生留有自由发挥的环境。比方说，在办公网络中可以采取对等式网络，而不必采取企业那种严格的域网络环境。

> 旧设备利用上：要尽可能地把学校的旧设备（如计算机、原有的一些办公室网络）加入到网络中，因为学校的经费普遍存在紧张的现象。因此，尽可能地为学校节省资金，也应该是网络组建实施方案上应该考虑的一个重点。

> 维护管理上：学校的网络管理人员一般都是从教师队伍中抽调，很少会外聘专业的技术人员。因此，无论是中央节点、服务器或管理软件上，都要尽量采取智能化、实用化的产品，让非专业的教师也可以轻松把握整个校园网络。

6.2 校园网设计方案

无论校园网络的规模是大或是小，都应该在组建之前写一份详细的设计方案。如果一边组建一边想，难免会手忙脚乱、缺东少西。实际上，设计方案的成功与否都会直接影响到工程的建设质量，以及今后网络是否能够可靠运行，都与其有着直接的关系，因此要非常认真地进行系统性的规划。

6.2.1 设计方案

设计方案要在充分考虑到前面内容的前提下，力争把每个环节写透，如：

- > 每个设备的特点，以及配套软件的简介等；
- > 网络的扩大和升级环境；
- > 组网需要的工具、材料和软件；
- > 整个组网所需要的预算；
- > 防火、防盗、防损。

在撰写设计方案时要尽量做到面面俱到、考虑周全、有主有次。因为在施工过程中经常要回答各种提问，做到有备无患、成竹在胸，可以大大提升校方对施工方的信心。必要时，可以先做一份调查卷让校方提供答案，尽可能地做出一份适用于学校实际情况的实用型、可扩展型、高性能的网络设计方案。



注意

在撰写设计方案时，在布线部分可以参考《中国建筑电器规范》、《工业企业通信设计规范》、《中国工程建设标准化协会标准》、《综合布线用电缆、光纤技术要求》及《建筑与建筑群综合布线系统工程设计与规范》等国内标准。

在设计方案评审通过以后，一般是按照如下步骤建设校园网络：

- (1) 布线施工与测试；
- (2) 安装网络设备；
- (3) 安装计算机与操作系统；
- (4) 安装应用软件；

第六章 组建校园网

- (5) 编写校园网管理规范与注意要点；
- (6) 用户培训；
- (7) 投入运行。

校园网的建设过程本身并不复杂，复杂的是后期漫长的运行与使用过程。为了保证这个过程尽可能的稳定、高性能运作，编写网络使用手册以及对教师进行短期培训是非常有必要的。

6.2.2 学校网络设计方案

下面，以一个小学组建网络为例，讲解一下校园网的设计过程。首先，来了解一下学校的组网要求。该校需要在网络中实现：

- > 一个多媒体教室；
- > 每位校领导的办公室都接入网络；
- > 每个教师办公室接入网络；
- > 一个电子图书馆系统；
- > 将办公室的打印机接入网络；
- > 局域网通过 ADSL 接入因特网。

接着，需要根据学校建筑的实际情况，绘出信息点分布平面图。尽量确定计算机的准确数量、计算机与交换机（核心交换机）的最远距离等。



此小学共有三栋楼房，一栋是五层的教学楼，所有学生都在此楼上课，每间教室都有一台计算机；一栋是三层的办公楼，供学校领导和教师们进行办公；还有一栋是三层的综合楼，综合楼上有图书室、多媒体机房、实验室、中心机房等。

由于整个学校的网络规模较小，加之建筑间的距离都不超过 100 米，整个网络建设的费用不会太多，所以，对于环境相对恶劣的室外线缆来说，推荐使用光纤进行千兆网络的架设，以便为以后的网络升级做好铺垫。当然，由于要增加光

纤收发器，工程预算会相应的提高一些——光纤收发器的价格在 400~800 元左右。需要注意的是，如果是单模光纤，那么就要用到单模光纤收发器，如果是多模光纤，则要用多模光纤收发器。

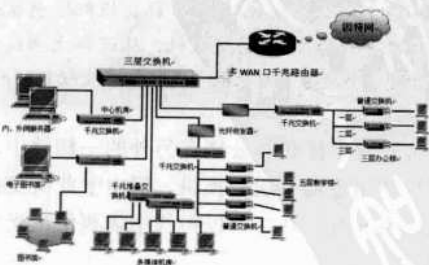


光纤收发器

光纤收发器有时也叫光电收发器，是一种将以太网的电信号和光信号进行互换的以太网传输媒质转换设备。即：它是一种以太帧的光电转换器（仅仅是信号转换，并没有接口协议的转换），它的电口和光口的传输都是以太数据。

对于面向外网的接口，建议使用多 WAN 口的千兆级路由器，以便为今后的外网速度升级做好铺垫——因为目前学校使用的还是比较落后的单 ADSL 接入。如果以后希望使用双 ADSL 接入，也可以很方便地实现，用不同的 WAN 口连接不同 ADSL 线路，再通过路由器自身的负载均衡或者路由策略等功能，可以实现线路的共用。当然，如果升级为光纤网络，也可以在路由器上很方便地实现。

在路由器后面建议使用三层交换机作为局域网的核心交换机，这样的设备可以在华为、H3C、锐捷等公司的产品中做出选择，如锐捷 RG-S3760 系列等。



网络拓扑



由于接入的因特网受 ADSL 设计使然，上行带宽极其有限，所以，面向外网的服务器只能接受极小流量的访问。因为使用了千兆路由器，所以，可以非常方便地对这方面的带宽进行升级。我们推荐花几百元购买虚拟主机面向外网用户开放网站、论坛服务，校内服务器仅在校内进行内部邮件、多媒体等服务。



下行带宽

由于图书馆和多媒体教室与中心机房都是在综合楼上，所以，使用低端的千兆交换机直接与三层交换机进行连接即可（由网络规模不大，因此可以考虑将汇聚层与接入层合二为一）。如果经费许可，推荐使用 H3C E126 系列这样的专为教育行业设计的产品。此外，由于多媒体机房有数十台计算机，所以需要使用堆叠交换机环境。



注意

堆叠 (Stack) 和级联 (Uplink) 是不同的两种交换机连接方法，它们的主要目的是增加端口密度。级联是通过集线器的某个端口与其它集线器相连的，如使用一个集线器 UPLINK 口到另一个的普通端口；而堆叠是通过集线器的背板连接起来的，它是一种建立在芯片级上的连接，如 2 个 24 口交换机堆叠起来的效果就像是一个 48 口的交换机，从逻辑上来说，它们属于同一个设备，因此优点是不会产生瓶颈的问题。

由于教学楼和办公楼在另外的一栋楼中，虽然可以使用低端二层交换机，但由于此类交换机一般没有光纤模块，所以布线中需要使用光纤收发器。

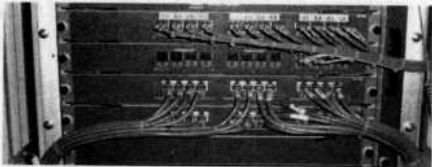
需要提醒的是，有些网络公司布线时只对室

外走线讲究整齐、美观，在教室的交换设备连线时就会随便使用端口，如图所示就是一个有 100 多台的多媒体教室连线情况。



零乱的布线

这样的连线在需要经常维护机房的校园网环境中，简直让后来的技术人员无从下手。正确的做法是将交换机的每一部分端口都规范到一批计算机，每一批计算机使用的网线都要用束线箍扎起以便识别。



规范的走线

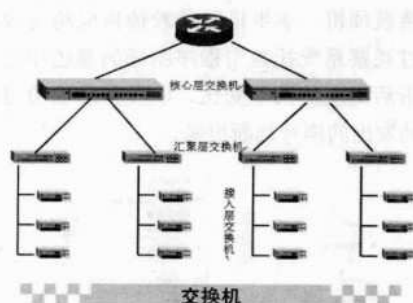
笔者的经验是不仅在每束线上都做标记，最好是在每根双绞线上都做标识，这样才能为今后的网络维护带来方便，这一点就好比写程序时在源代码后面添加说明文字一样。



在双绞线上做标记

上述网络结构是按照“核心层→汇聚层→接入层”这种业界通用的层次化网络设计模型的。

第六章 组建校园网



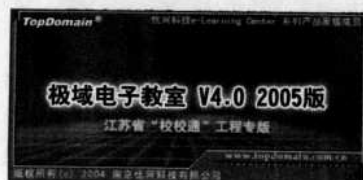
通常将网络中直接面向用户连接或用于访问网络的部分称为接入层，将位于接入层和核心层之间的部分称为分布层或汇聚层，接入层的目的是允许终端用户连接到网络，因此接入层交换机具有低成本和高端口密度的特性。汇聚层交换层是多台接入层交换机的汇聚点，它必须能够处理来自接入层设备的所有通信量，并提供到核心层的上行链路，因此汇聚层交换机与接入层交换机比较，需要更高的性能、更少的接口和更高的交换速率。通常，将网络主干部分称为核心层，核心层的主要目的在于通过高速转发通信，提供油画，可靠的骨干传输结构，因此核心层交换机应拥有更高的可靠性，性能和吞吐量。

6.3 多媒体教室

信息化环境的构筑根本目的就是为教学服务，因此课堂信息化教学环境的建立应该是校园网建设的一个重要目标。在校园网络组建多媒体综合教室，不仅可以满足正常的辅助教学活动，还可以用来举办讲座、开展培训。

6.3.1 电子教室概述

在多媒体教室硬件安装完成后，必须安装相应的多媒体教室管理软件。在本书中使用的是“极域多媒体电子教室 V4.0 江苏省校校通专用工程版”。



多媒体电子教室软件

先来了解一下软件的特点：

> 班级模型可根据教室不同情况随意拖动更改，并自动保存。

> 屏幕广播效率极高，尤其在网络条件较差时亦能体现出良好的性能；可以根据网络条件调节网络补偿强度，根据广播内容调节广播及录制效率，使广播达到最佳效果，可以广播多媒体课件。

> 语音广播，VCD 广播可以达到学生机与教师机同步，无任何延迟。

> 当教师在未锁定学生机键盘、鼠标情况下广播或回放时，学生可以利用智能滚动的窗口模式接收广播，此模式可以使学生轻松地跟着教师进行同步操作，边看边练习，使学习由被动转为主动。

> 教师广播教学和语音教学时允许学生发言，并可方便地切换发言学生；可随时方便地使一组学生加入或退出教学行列。同时屏幕广播的性能大大提高。

> 分组教学将学生分为若干小组，由组长代替教师进行各项功能操作，使教学过程更生动。

> 将学生分为若干小组进行语音讨论，各组之间互不干扰。

> 作业提交可以方便学生递交电子文件作业。

> 电子点名可以通过让学生签到来实现电子点名。

> 网络影院能够播放几乎所有格式的视频文件。

> 巧妙地将学生演示与监控转播结合在一起，使教师与学生的交互更加自然、灵活，遥控时教师可以与被遥控学生协同工作。

> 屏幕录制与电子教鞭结合使用可以实现电子备课。

> 文件分发功能强大且接口相当易用，可以定义宏目录。

> 教师可通过视频直播功能将实时视频信号通过网络同步传输给所有学生机，能从根本上满足跨网段教学的要求。

极域电子教室 V4.0 主要由教师机安装的管理端和学生机安装的客户端组成，功能有如下这些

教师机：广播教学、语音教学、语音对讲、

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

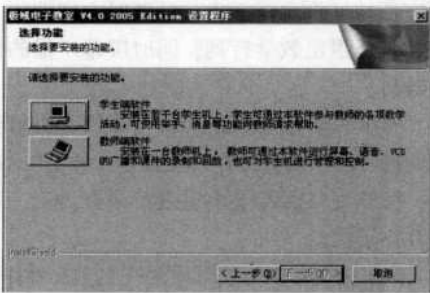


学生演示、监控转播、屏幕录制、屏幕回放、分组教学、语音讨论、视频直播、黑屏肃静、网络影院、文件分发、查看作业、电子教鞭、电子点名、班级模型、系统设置、远程命令、远程设置、远程消息、清除举手、清除未登录学生机、查看学生属性、系统锁定、可选窗口显示模式。

学生机：电子举手、远程消息、电子签到、提交作业、窗口接收广播、可选窗口显示模式。

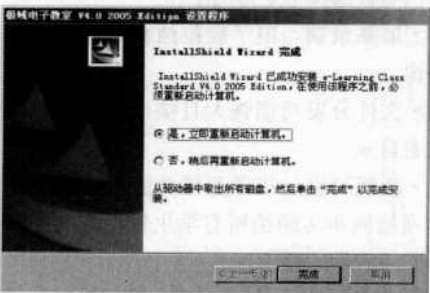
6.3.2 软件的安装

这款软件分别需要在一台教师机和若干台学生机中安装，安装软件是同一个。在安装过程中进入如图所示的界面时需要做出选择。在本例中，教师机安装了 Windows Server 2003 系统、学生机分别安装 Windows 2000 和 Windows XP 等系统。



选择安装的类型

程序安装到硬盘中需要 35MB 左右的空间，在安装完成后需要根据提示重启计算机。学生机和教师机安装后的不同之处在于，教师机中需要手工运行管理端程序。学生机是强制、自动运行客户端程序。



安装完成

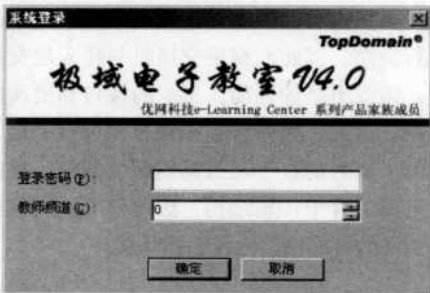
根据安装经验，应在安装完所有的学生机后

再安装教师机。学生机登录教师机成功与否，可以通过观察系统托盘中程序图标的颜色变化、右键单击后出现的菜单变化，以及登录成功与退出后自动发出的声音判断出来。



学生机登录前后的菜单状态

在教师机完成重启后需要双击桌面上的“极域电子教室教师机”图标，在出现如图所示的对话框时，默认的登录密码为空，频道号可以设置为 0 ~ 99 之间的任何整数。



登录对话框

在保持默认设置并单击“确定”按钮后，就可以进入教师机的操作平台。



教师机程序运行界面

因为只启动了三台学生机，所以程序中只会立即找到这三台计算机，并分别在右侧生成计算机列表，以及在左侧的窗口中显示学生机的屏幕缩略图。

选中任意一个缩略图并单击下方的“屏幕监看”按钮，可以即时调看该学生机的屏幕画面，从而对学生的操作了如指掌。如果不选缩略图就单击此按钮，则会出现如图所示的状态，即可以对所有学生机的屏幕进行监控。



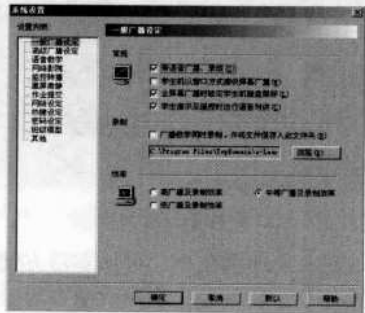
监看学生机屏幕

在教师机的程序标题栏右侧有四个按钮，如果要对程序的初始环境进行设置，需要单击左侧第一个按钮。



标题栏

稍后，将会弹出如图所示的窗口，在这里可以对程序的各个方面进行设置。比方说，在默认的“一般广播设定”界面中可以对广播教学环境进行设置等等。



程序设置

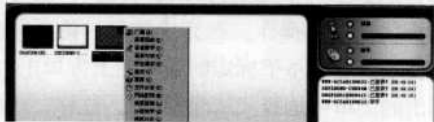
具体的设置方法请见程序说明书，此处略。因为此类的软件在功能上基本都是大同小异，所以，本书将只讲解通用的几项主要功能。

6.3.3 联机讨论

在电脑课开始以后，一般情况下教师都是简单地讲几句学习要点，然后就由学生自习了。在学生的过程中，学生可以随时通过电子教室软件就某个问题和教师进行联机讨论。具体的实现方法是：

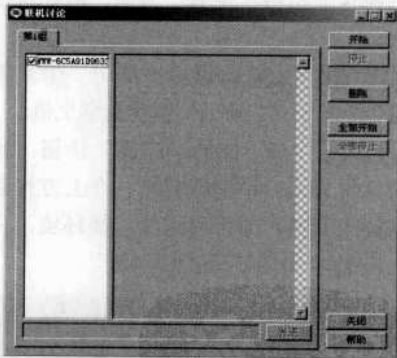
STEP 1 学生在自己的计算机中，右键单击屏幕右下角系统托盘中的电子教室图标，在弹出的菜单中选择“举手”。

STEP 2 在教师机中的电子教室软件里，该学生的屏幕缩略图右上角将出现一个举手的标志，并在右侧的消息框中出现相应的提示。



举手

STEP 3 在举手学生机的缩略图上方单击右键，在弹出的菜单中选择“联机讨论”。在弹出如图所示的对话框时，在左侧的学生机列表中将会自动勾选举手的学生机。



联机讨论对话框

STEP 4 单击“开始”按钮后，学生机中将会弹出“联机讨论”对话框。此时，双方即可在各自的“联机讨论”对话框下方的文本框中输入各自的发言内容。在联机讨论的过程中，学生可以单击“申请发言”按钮进行语音发言。



开始讨论

这个联机对话框的启动与退出是由教师机控制的，在学生机中无法进行关闭操作，但可以进行最小化和还原操作。在完成联机讨论后，教师需要在本机中有举手标志的缩略图上方单击右键，在弹出的菜单中选择“清除举手”。这样，才能彻底结束本次的联机讨论。

6.3.4 广播教学

广播教学功能可以将教师机屏幕和教师讲话传送到学生机屏幕上，这项功能可以协助教师把自己的操作演示给学生看。为此，需要执行如下操作：

STEP 1 在缩略图窗口中选中一个或多个屏幕，也可以按下“Ctrl+A”键全选学生机。

STEP 2 单击下方的“广播”按钮，此时电子教室软件将会自动隐藏起来，在上方将会出现一个快捷工具条。如果要退出广播环境，只需单击工具条上的“广播”按钮即可。



快捷工具条

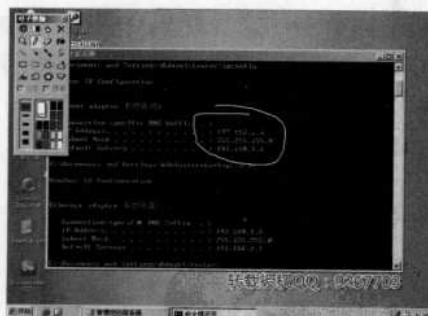
STEP 3 此时，被选中的学生机屏幕将会以窗口的形式出现教师机的屏幕画面，并在耳机中可以听到教师的声音。



学生机中的广播窗口

STEP 4 建议在教师机的程序设置中允许学生机在广播时使用鼠标和键盘，否则，学生机中就没有办法调节这个广播窗口的大小和位置了，以及无法根据教学内容立即进行相应的实习操作了。

在广播教学中，教师随时可以在工具条中单击“教鞭”按钮，在屏幕上进行一些重点标注、注解等操作，此外也可以配合投影仪进行电子板书或屏幕注解。



电子教鞭

通过左上角的调色板，可以非常方便地更改教鞭墨迹颜色。比方说，在对“命令提示符”中的命令进行讲解时，就可以使用白色。

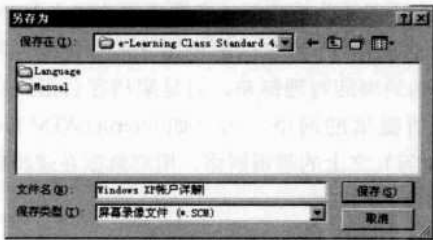
6.3.5 屏幕录制与回放

绝大多数的时候，同样的一节课内容需要反复复的讲上几年。教师通常会讲到麻木，再无

第六章 组建校园网

激情可言。利用屏幕录制功能，可以将教师讲得最好的一节课实况录制下来，通过反复播放可以让激情永在，进而让教师有更多的时间对学生进行辅导。要使用这项功能，需要执行如下操作：

STEP 1 单击下方的“屏幕录制”按钮，在弹出的如图所示对话框中，需要为录制产生的文件起一个名字，并选择合适的保存位置。



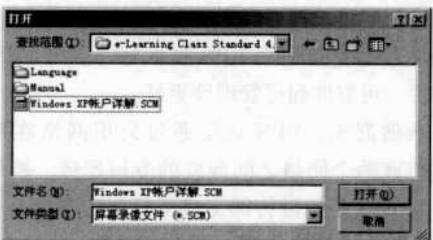
保存文件

STEP 2 单击“保存”按钮后，电子教室程序的窗口将会自动最小化。此时，就可以进行各种演示了。在演示完成以后，单击工具条中的“录制”按钮即可结束录制任务。



工具条

STEP 3 以后，在教师机随时都可以单击“屏幕回放”按钮，在弹出的如图所示对话框中选择录制的视频进行课程回放，教师由此可实现电子备课。



选择要回放的视频

6.3.6 文件分发

“文件分发”功能允许教师将教师机里的一个或多个目录、文件，发送至所选学生机的指定目录下，若该目录不存在则自动新建此目录，若文

件已存在则自动覆盖原始文件。以教师在讲解数据库软件 Access 的应用时，希望把 book.mdb 这个文件发送到每个学生的 D 盘分区为例，需要执行如下操作：

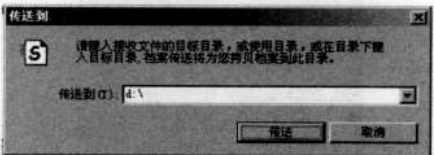
STEP 1 选中要发送文件的学生机并单击“文件分发”按钮，如果直接单击此按钮则表示向所有的学生机中发送文件。

STEP 2 在弹出的如图所示对话框中，在上方选中要发送的文件并单击“加入”按钮，将其添加到下方的待发送列表。



选中文件

STEP 3 单击“传送”按钮并在弹出的如图所示对话框中，指定或手工输入一个在学生机里用于存储传送文件的路径。



指定路径

STEP 4 单击“传送”按钮后，在窗口的右下角将会看到文件传送的进度。



传送进度

STEP 5 传送完毕以后，学生机中将会自动弹出如图所示的对话框，在其中可以看到传送的文件名称、路径等信息。



如果只出现了提示框，却没有任何内容，则表示传送失败。失败原因可能是：

- > 若盘符不存在或路径非法则不允许分发；
- > 若磁盘空间不足的学生机将无法接收分发文件；
- > 若指定的分区不可用，也无法传送文件。

6.3.7 远程命令

有时候，为了统一学生机的操作，需要对学生机发送统一的操作指令。比方说，可以通过发送一个打开记事本的指令，让所有或选中的学生机中自动运行“记事本”程序。



在电子教室程序中，提供了比较完善的远程命令供教师选用，具体的操作就不再细述了。

上述内容就是极域电子教室在多媒体机房的部分功能应用实战，限于本书篇幅就不再一一细述其它的功能了。

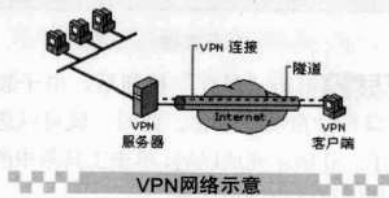
6.4 VPN的实现

VPN 即“Virtual Private Network”的简称，中文是“虚拟专用网络”的意思。它提供了一个

通过公用网络（Internet 或其它公共互联网络）安全（使用加密技术）地对内部网络进行远程访问的连接方式。VPN 技术从 2002 年开始得到了飞快的发展，被认为是未来几年网络发展的一个重要方向。

6.4.1 VPN概述

之所以称为虚拟网，主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台（如 Internet,ATM,Frame Relay 等）之上的逻辑网络，用户数据在逻辑链路中传输。



由于通过公用 IP 网络来建立 VPN，不再需要铺设专门的线路进行通信，这样就可以节省大量通信费用，可称得上物美价廉。现在教育系统大力推行的城域网，实际上就是为了实现内部网络的安全性访问而组建的。对于无法投入巨大资金铺设线路的一般性企业来说，大多都是采用租用电信运营商的线路，如光纤、SDH 和 DDN 等实现专用网络。这样做虽然已经节省了很多费用，但仍然没有自行使用 VPN 技术好，因为 VPN 的安全性、可靠性和可管理性更好。

概括起来，VPN 就是通过公用网络在两台计算机或两个网络之间建立的专用连接。换言之，VPN 就是把因特网变成了模拟的专用 WAN。根据 VPN 所起的作用，可以将 VPN 分为 3 类，即 VPDN、Intranet VPN 和 Extranet VPN。其中，Intranet VPN 技术最为常用——在本书中讲解的也是这种技术。

Intranet VPN 主要指的是在分支机构 LAN 和总部 LAN 之间的 VPN。通过 Internet 这一公共网络将各地分支机构的 LAN 连到总部的 LAN，以便内部的资源共享、文件传递等，可节省 DDN

第六章 组建校园网

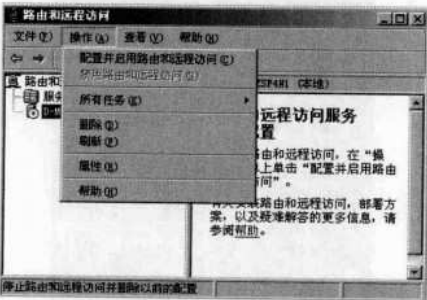
等专线所带来的高额费用。很明显，VPN 技术不仅仅可以在学校网络中使用，因为越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司和研究所等，各个公司之间传统的网络连接方式一般是租用专线。利用 VPN 特性可以在 Internet 上组建世界范围内的 Intranet VPN。利用 Internet 的线路可以保证网络的互联性，而利用隧道、加密技术等 VPN 特性可以保证信息进行安全传输。

6.4.2 VPN实例

现在，让本书以一个实例的方式讲解如何实现学校的 VPN 网络建设。例举：某学校在城市的另一个区设立了 A 分校，现在 A 分校需要时时访问总校内部的网络，以查阅、下载一些内部资料，那么，这就是个“远程用户通过 Internet 访问学校内部网络”的过程，显然“网络访问路径”需要两层，即 Internet 和内部网络。这个时候，就可以使用 VPN 服务来解决两层访问的问题了。下面让我们来看看如何配置：

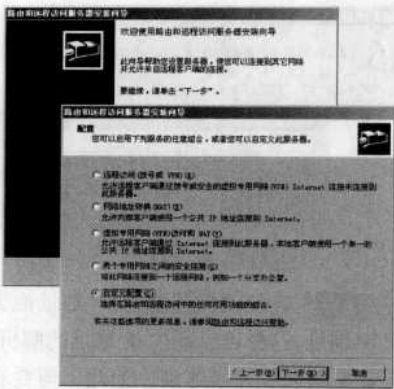
1. 配置VPN服务器

STEP1 依次单击“开始”→“程序”→“管理工具”→“路由和远程访问”菜单，在打开的“路由和远程访问”服务窗口中，选中控制台中的 Hostname（本机名称）并依次单击“操作”→“配置并启用路由和远程访问”菜单。



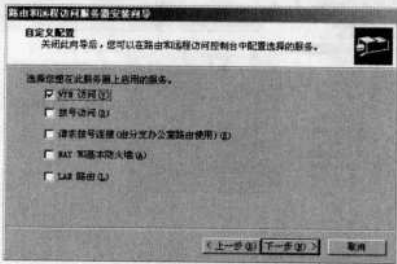
路由和远程访问

STEP2 在弹出的安装向导中单击“下一步”按钮，在“配置”对话框中选择“自定义配置”选项后继续。



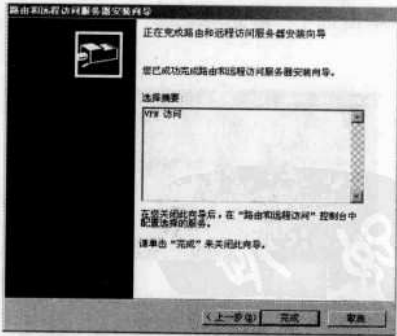
向导窗口

STEP3 在“自定义配置”对话框中勾选“VPN 访问”项后继续。



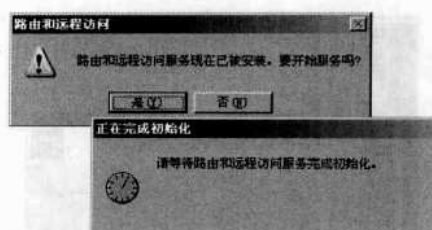
勾选“VPN访问”项

STEP4 在出现如图所示的界面时，直接单击“完成”按钮。



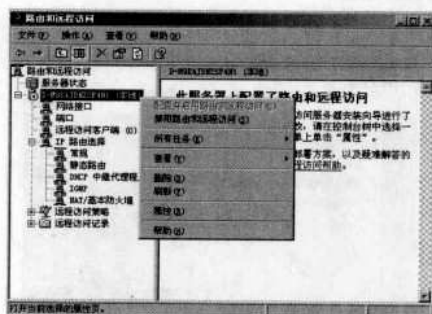
完成界面

STEP5 在弹出的“路由和远程访问”对话框中单击“是”按钮，等待几秒钟后，待路由和远程访问服务完成初始化操作后 VPN 服务器即可启动了。



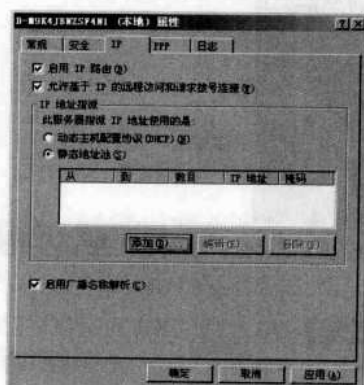
启动VPN服务器

STEP 6 现在需要使用静态 IP 地址池为拨入端分配 IP 地址,这样可以减少 IP 地址的解析时间,从而有效提高远程连接速度。为此,需要右键选中并单击控制台中的服务器名,在弹出的菜单里选中“属性”菜单。



选择属性

STEP 7 打开“hostname (本地)”属性窗口,单击切换至“IP”选项卡设置界面。在“IP 地址指派”选项中单击选中“静态地址池”后,再单击“添加”按钮。



单击“添加”按钮

STEP 8 在弹出的“新建地址范围”对话框中,

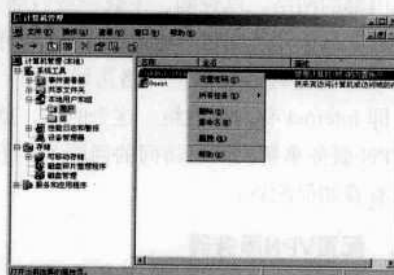
在“起始 IP 地址”和“结束 IP 地址”右侧的 IP 地址栏中键入所需的内部网络的 IP 地址范围 (如 192.168.1.15~192.168.1.21)。

2. 添加权限账号

在服务器配置完毕后,还需要为远程的用户添加一个能够拨入 VPN 服务器的权限账户,VPN 服务器将使用该账户对远程连接进行认证。为此,需要执行如下操作:

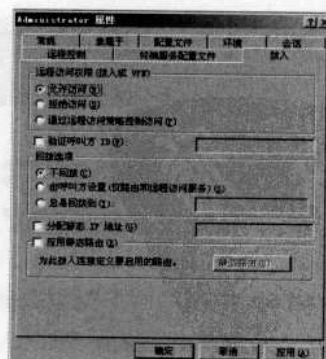
STEP 1 右键单击“我的电脑”图标,并在弹出的菜单中选择“管理”。

STEP 2 在打开的“计算机管理”窗口中展开“本地用户和组”→“用户”项,右键单击用户列表中的某一个用户名称 (如 Administrator),在弹出的菜单中选择“属性”。



选择属性

STEP 3 在打开的“Administrator 属性”窗口中单击切换到“拨入”选项卡设置界面,单击勾选“远程访问权限”部分的“允许访问”选项。



设置允许访问

STEP 4 设置完毕后,单击“确定”按钮后就结束了服务器与账号的设置操作了。

第六章 组建校园网

3. 配置VPN客户端

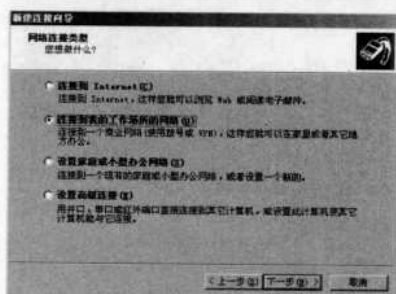
由于目前使用 Windows XP 系统的用户比较多，所以下面就以 Windows XP 操作平台为客户端环境，讲解一下 VPN 客户端的配置方法。为此，需要执行如下操作：

STEP 1 双击“控制面板”中的“网络连接”项，在打开的“网络连接”窗口中双击左侧“网络任务”区域的“创建一个新的连接”链接。



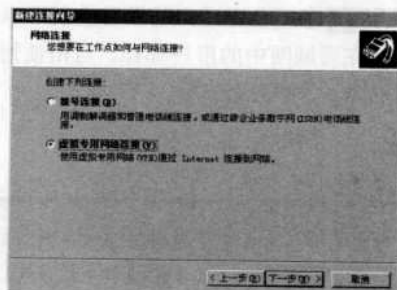
创建一个新的连接

STEP 2 在弹出的“新建连接向导”进行到“网络连接类型”对话框时，点选“连接到我的工作场所的网络”选项继续。



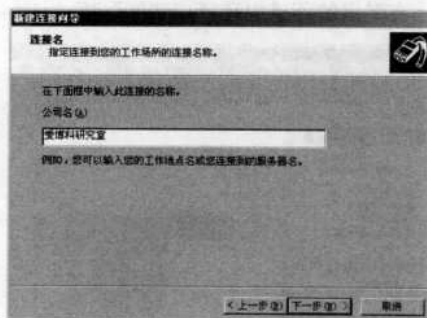
点选“连接到我的工作场所的网络”项

STEP 3 出现如图所示的“网络连接”对话框时，选择“虚拟专用网络连接”项继续。



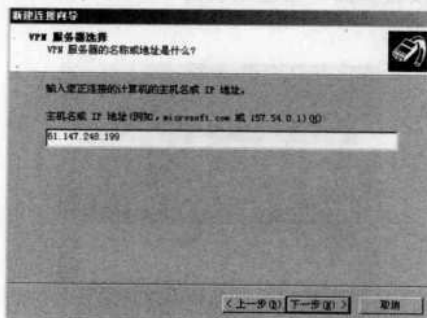
选择“虚拟专用网络连接”项

STEP 4 出现如图所示的“连接名”对话框时，键入一个连接名称后继续。



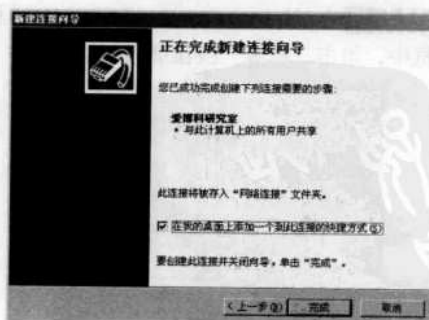
输入名称

STEP 5 在“VPN 服务器选择”对话框中，键入 VPN 服务器端的 IP 地址或域名后继续。



输入IP地址或域名

STEP 6 最后一步中勾选“在桌面上创建此连接的快捷方式”后，单击“完成”按钮结束创建过程。



完成设置

STEP 7 为了避免出现成功连接 VPN 服务器后，客户端不能访问 Internet 的问题，还需要对刚

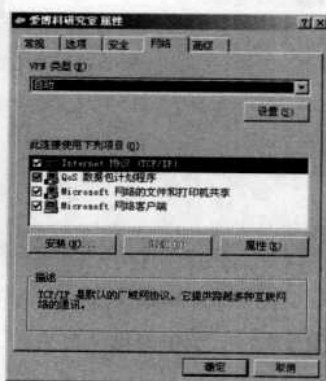


刚创建的“VPN 连接”做简单的配置。为此，需要在“网络连接”窗口中右键单击刚创建的链接图标，在弹出的菜单中选择“属性”项。



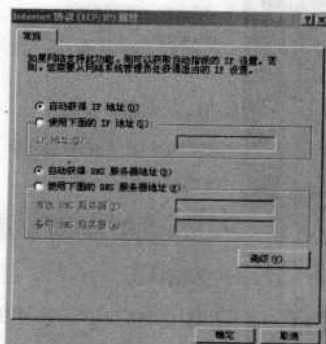
选择属性

STEP 8 在弹出的窗口中切换到“网络”选项卡设置界面，在这里双击“Internet 协议 (TCP/IP)”项。



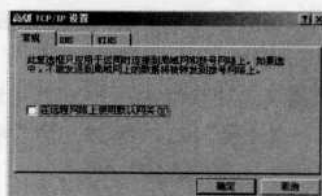
选择TCP/IP协议

STEP 9 在“Internet 协议 (TCP/IP) 属性”对话框中，单击“高级”按钮继续。



单击“高级”按钮

STEP 10 在随即出现的“高级 TCP/IP 设置”对话框中，清空“常规”选项卡设置界面中“在远程网络上使用默认网关”项的选中状态。



清空选项

4. 拨入VPN服务器

现在远程用户就可以使用被赋予拨入权限的用户名“administrator”拨入 VPN 服务器了。具体的实现过程如下：

STEP 1 双击桌面上的 VPN 连接图标弹出拨号窗口，在“用户名”和“密码”栏中输入相应的信息，并单击“连接”按钮即可与 VPN 服务器建立连接了。



开始拨号

STEP 2 连接成功后，远程用户就可以如同服务器所在局域网中的用户那样，自由使用局域网内的资源了，如网上邻居、FTP 等。



注意

成功建立连接后，客户端在访问服务器端的共享资源时可能会出现长时间的搜索过程。这时可以使用“搜索计算机”功能对指定计算机进行搜索。

第七章 组建无线局域网

在如今这个处处“移动”的世界里，传统的有线局域网（LAN）已经越来越不能满足人们的需求了！在无线网络迅猛发展的今天，无线局域网（WLAN）已经成为可应用在家庭、企业中的一种成熟的网络了。摆脱线缆的羁绊，自由自在地在网络的天空中翱翔——这就是无线的魅力！无线局域网（Wireless Local Area Network, WLAN）的应运而生无疑是场及时雨。

在本章中，就将和读者们一起聚焦无线，把握无线的脉搏，紧紧地握住无线的手。

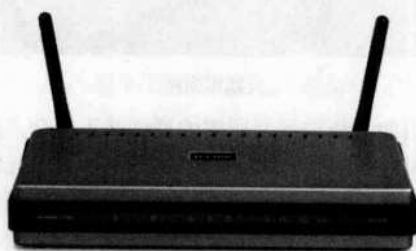
7.1 无线局域网基本知识

当无线网卡已经成为计算机的标配硬件时，在家庭、企业、学校等各种网络环境中，无线技术似乎已经无所不在了……作为已经非常成熟的网络技术，无线网络正在以它的高速传输能力和灵活性发挥着日益重要的作用！

7.1.1 什么是无线局域网

顾名思义，无线局域网（WLAN）就是使用无线电波作为传输介质的局域网，它适用于难以布线或布线成本太高的环境。因此，有人形象地比喻说：未来的空中到处都是数据。

目前，组建网络的传输介质主要依赖于双绞线或光纤。有线网络的优点是传输质量好，不足是布线工程量大、线路较容易受损、网中的各个节点不可移动等等。在支持 802.11N 技术的网络设备广泛应用之前，无线网络只能做为弥补有线局域网不足、起到网络延伸效果的一种辅助型网络。如图所示是支持 802.11N 技术的 D-Link DIR-625，使用它能够架设出传输速率高达 300Mbps 的无线网络。



D-Link DIR-625

如今，随着无线网络的日趋高速化，无线技术也可以轻松、独立地组建出大型网络了。目前，主流的无线局域网标准还是使用 802.11G 和 802.11B，速度在 11Mbps/s、54Mbps/s、108Mbps/s 之间。无线局域网特别适合在小型局域网中使用，因为它的信号覆盖范围在小型局域网中显得最为强劲。

当然，如果有必要也可以通过购买 D-LINK DWL-1750 250mw 这样的室外大功率无线路由，实现在数百米的强大信号覆盖。



大功率无线路由

对于大型企业、山区这样的环境，还可以使用价值几千元的远端网桥设备组建无线网络，这样的设备信号可覆盖 25 公里的 D-Link DWL-1800R 室外大功率网桥等。



大功率网桥

组建无线局域网所需的硬件并不复杂，少则使用两块无线网卡（无线网络产品都自含无线发射/接收功能）即可，多则可以使用多个无线路由配合组网。需要选用什么无线设备，要看无线网络的规模后再定。

与有线网络相比，无线局域网主要具有以下几个优点：

> 安装便捷。在有线网络建设中，施工中往往需要破墙掘地、穿线架管，而无线局域网最大的优势就是能够免去或减少网络布线的工作量。一般只要安装一个或多个无线网桥设备，即可以建立覆盖整个建筑或地区的无线局域网。

> 移动灵活。在有线网络中，即便是笔记本电脑，其上网时摆放的位置也要受网络接入点所在位置的限制，而无线局域网络在建成后，只要是配有无线网卡的电脑，就都可以在无线网络的信号覆盖区域内的任何一个位置接入无线网络。

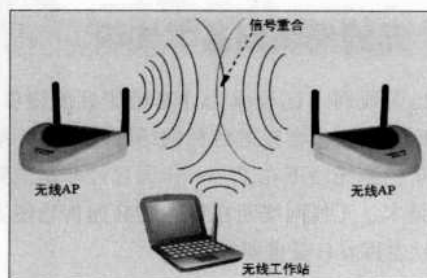
> 经济节约。在使用方面，无线局域网的机

动性、便利性，是有线网络所不及的；在成本上，它同样可以节省下可观的线缆费用。

> 易于扩展。无线网络中，可以随时轻松增添无线网桥，这可以使无线局域网内的无线用户成倍增加——从信号稳定的角度来看，每增加一个无线设备，就意味着可以成倍增加数十乃至上百个无线工作站接入无线网络。而有线局域网中，如果要增加如此数量的接入口，光是布线这一点就会让人头痛不堪了。

7.1.2 无线漫游概述

由于无线电波在传播过程中，会随着距离的延伸而不断衰减信号强度。为了改善这种不足，通常需要使用多个无线设备来实现无线信号的无缝覆盖和重合，只要无线路由或无线 AP 群的设置正确，无线工作站就可以自由地漫游在如图所示的无线电波所能覆盖的区域。



无线信号的无缝覆盖和重合

无线网卡能够自动发现附近信号最好的无线路由或 AP，并能通过这个其收发数据，从而保持不间断的网络连接，这就是无线漫游（Roaming）技术。显然，无线漫游的目的就是用于扩展无线信号的覆盖范围，从而保证无线用户的信号不会轻易中断。

注意

对于无线路由、网桥等设备而言，有效传输距离是相当重要的。需要注意的是，不要被产品包装盒上的说明给迷惑了，说明中的“最大传输距离”的数值，大多是在没有任何遮挡物的条件下计算出来的，只是个理论数字而已。在钢筋混凝土浇注的高楼大厦中，我

第七章 组建无线局域网

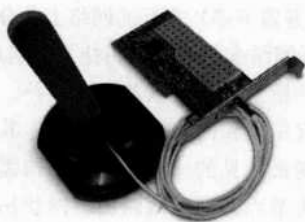
们更应该看重无线路由器的信号穿透能力。大多数高品质产品可以做到在 30 米之内穿越两堵厚厚的墙壁，而少数低端产品可能连一个小小的室内“拐弯”，即便开着门，也无法与另一间房间中的无线客户端完成通信。

7.1.3 无线局域网的构件

无线局域网作为网络发展的一个重要方向，它已经得到了广大网络设备生产商的大力支持，目前可以购买到的无线网络产品很多。下面，让我们花上几分钟对它们加入解。

一个小型无线网络的硬件设备主要包括四种，即无线网卡、无线路由和无线天线。由于无线网卡在前面的内容中已经介绍过了，所以，下面只介绍无线路由和无线天线。

仅凭无线网卡也可以组建无线局域网，只有当需要扩大无线网络规模时、需要将无线网络与传统的局域网连接在一起，或者需要实现无线网络的 Internet 共享接入时，才需要使用无线路由。当无线路由与计算机的距离较远，信号变得较差时，可以通过更换或增加无线天线放大信号，以便接收更远距离的无线信号，从而延长无线网络的覆盖范围，如图所示是室内天线。



无线天线

当计算机与无线路由等无线设备相距较远时，随着信号的衰减，传输速率会明显下降，或者是根本无法实现通信。此时，就必须借助于无线天线对所接收或发送的信号进行增强。无线天线有许多种类型，常见的有室内天线和室外天线两种。

有的无线路由中还内置了无线打印服务功能，只要把打印机的 USB 线跟机器后面的 USB 接口相连接，并放在大家方便共用的位置，然后通过

对电脑进行简单设置，就可以实现多台电脑无线共享一台打印机了。



无线打印机接口

此外，也有一些独立的无线打印共享器可以用于接驳于打印机的并行口，从而实现无线网络与打印机的连接，使无线网络中的计算机能够共享打印机。



无线打印共享器

构建小型无线局域网的硬件设备主要是上述几种，还有一些适用于有线电视、卫星、VOIP 的无线产品，因为在小型无线局域网中不常用，就不再一一介绍了。

目前，市场上无线产品很多，在选择时要注意如下几点：

* 标准的选择，不同的标准决定不同的传输性能。

根据无线通信协议 IEEE802.11 协议族中各个协议的特点，在购买设备时，应该在经费允许的前提下尽可能选择支持传输速率高、传输距离长的



协议。推荐购买支持 IEEE802.11n 的无线设备，如 D-Link DIR-625 等。如果经费紧张，也可以购买支持 IEEE802.11g 的无线设备，如 D-LINK DSL-G664T 54M 无线路由、D-LINK DI-784 108M 无线路由、D-LINK DI-624+ 54M 无线路由等。

* 品牌的选择，不同的品牌决定设备的整体品质。

无线网络设备大致可以分为三大阵营：一是美国产品，如 LINKSYS、AVAYA、3COM 等，这类品牌的产品具有品质优良、工作稳定、性能出众、管理方便等特点。但是，其价格往往较高；二是台湾产品，如 D-LINK(友讯)、ACCTON 等，其制作工艺、产品性能也相当不错，具有非常高的性能价格比；三是大陆产品，如清华比威、TP-LINK(普联)等，其产品质量也不错、价格也很便宜，很适合小型办公网络使用。

* 人性化设计，不同的设计决定设备的易用性。

在人性化设计方面，我们可以从管理设计、天线设计两个方面来简单对比一下。

(1) 管理与易用性。无线产品作为一个网络设备，自然需要相应的管理功能。有些无线局域网产品的安装维护比较复杂，非专业技术人员往往很难完成驱动及其它方面的安装，而有些无线产品的安装维护却比较简单，这一点对于家庭用户来说尤应注意。

(2) 天线的拆卸。天线的拆卸便于我们更换增益天线。无线路由受电源和信号长度所限，不一定总是处于信号发射的最有利位置，这时可以考虑在无线路由上安装形态各异的增益天线，这样一来就可以大大增强信号的有效覆盖范围。

* 安全设计。

为了保证网络安全，现在的无线路由器大多配备了安全管理功能，如防火墙等。虽然这种硬件防火墙不可能阻挡所有的攻击，但是对于防止黑客攻击还是有一定效果的，而且还能不占用系统资源。



安全功能

7.2 组建最简单的无线对等网络

不同类型的无线网络具有不同的特点，使用不同的设备可以适应不同类型的用户。因此，在动手搭建无线网络之间，一定要先搞清楚自己的现状、搭建网络的目的、想要实现的功能、对传输速率的要求，以及准备投入的资金。

7.2.1 拓扑结构与传输介质

在组建网络时，通常会用网络的拓扑结构来分类。拓扑 (Topology) 即网络组件的物理 (真实) 或逻辑 (虚拟) 分布形式。根据这个定义，我们可以将拓扑看成是“许多节点 (是计算机、网络打印机、服务器等等) 在互通网络上的分布形式”。目前，有线网络有五大网络拓扑，分别是总线型、令牌环状、星型、树状以及网状拓扑。在无线网络中，只有星型和网状这两种拓扑。其中，星型拓扑是目前最常见的一种，这种结构需要包含至少一个中央节点，即无线路由。网状拓扑和星型拓扑有些不一样，主要是网状拓扑并没有中央节点。每个节点都可以与同在一个网段的其它计算机自由沟通。

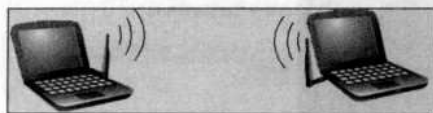
在实际应用中，无线网络的组网方案中主要有以下几种：

1. 对等无线网络

如图所示的对等无线网络只使用无线网卡即可构成。因此，仅仅在每台计算机上插上无线网卡，再加以简单的软件配置，即可实现计算机之间的

第七章 组建无线局域网

无线连接，并构建最简单的无线网络，进而可以使用无线信号在计算机之间共享资源。

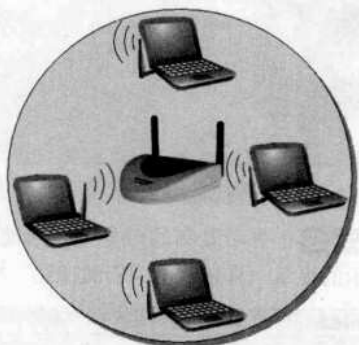


双机互联

由于无线对等网络的传输距离有限，所有的计算机之间必须在有效传输距离内。否则，根本无法实现彼此之间的通信。因此，这类网络的覆盖范围非常有限。另外，由于所有计算机之间都要共享连接带宽，所以只适用于接入计算机数量较少、并对传输速率没有较高要求的小型无线网络。

2. 独立无线网络

所谓独立无线网络，是指借助无线路由构成的无线网络。从如图所示中可以看出独立无线网络使用了一个无线路由和若干无线网卡。



独立无线网络

独立无线网络方案与对等无线网络所不同的是：独立无线网络方案中加入了一个无线路由。无线路由可以对网络信号进行放大处理，一个工作站到另外一个工作站的信号都可以经由该无线路由放大并进行中继。只要在无线路由覆盖范围内，无线移动工作站就可以实现彼此之间的通信。



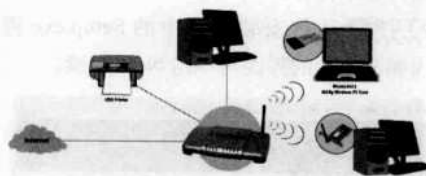
注意

由于无线路由的覆盖范围是一个圆形区域，因此，

无线路由应当尽量放置在无线网络的中心位置，而且各无线客户端与无线路由的直线距离最好不要超过 30 米，也不要穿越过多的楼板和墙体，以避免因无线信号衰减过多而导致通信失败。

3. 混合无线网络

由于无线路由通常会提供一个或几个以太网口，因此既可连接无线网络，又可连接以太网，并可以作为网桥实现两者之间的相互通信。这种如图所示的无线和有线并存的网络，即可称之为混合无线网络。



混合无线网络

4. 无线漫游网络

无线漫游网络可以利用以太网将多个无线路由连接在一起，从而实现无线信号的无缝覆盖。当无线用户遭遇一个无线访问点的信号变弱，或因为无线访问点由于通信量太大而拥塞时，可以不中断与网络的连接，这一点与我们平时使用的移动电话非常相似。

由于多个路由信号覆盖区域相互交叉重叠，因此，各个路由覆盖区域所占频道之间必须遵守一定的规范，邻近的相同频道之间不能相互覆盖，否则会造成路由在信号传输时的相互干扰，从而降低路由的工作效率。

7.2.2 双机无线组网实战

本书推荐读者们使用 Windows XP SP2 组建无线局域网。因为这个操作系统版本对无线网络提供了良好的支持，可以让用户非常容易地完成无线局域网的配置。下面，让我们来学习两台计算机中，通过安装无线网卡实现无线局域网的方法。

1. 安装无线网卡

与安装其它所有硬件一样，当在计算机中插

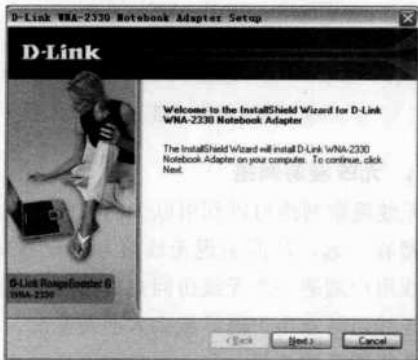


入无线网卡时（不管是 PCMCIA 卡或 USB 卡），Windows XP 都会弹出如图所示的“发现新硬件”的提示。



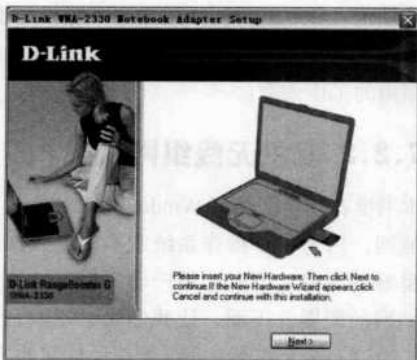
接下来，会遇到两种情况，一是如果当前插入的无线网卡驱动已经在 Windows XP 中内置了，那么就会自动安装好相应的网卡驱动程序。否则，需要运行购买网卡时附带的安装程序进行驱动的安装。以安装 DLink WNA-2330 无线网卡为例，需要执行如下操作：

STEP 1 运行安装光盘中的 Setup.exe 程序，在出现如图所示的界面时单击 Next 继续。



安装向导

STEP 2 根据图中的提示，将无线网卡插入到笔记本电脑中。



安装网卡提示

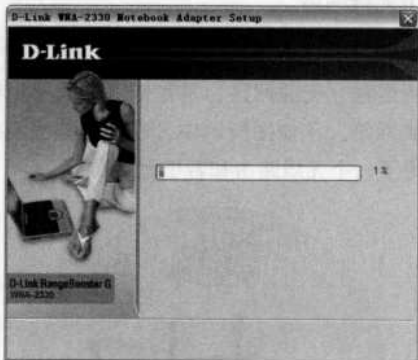
STEP 3 在自动检测到以太网卡后，将会自动弹出如图所示的对话框。在这里建议选择“否，

暂时不”项继续。



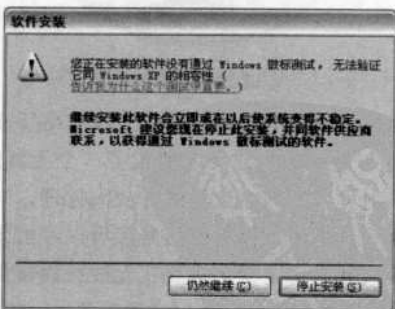
新硬件向导

STEP 4 接下来，耐心等待安装向导完成驱动文件的复制。



复制驱动文件

STEP 5 在驱动复制的过程中，可能会出现如图所示的提示，直接单击“仍然继续”按钮。



安装提示

STEP 6 在完成驱动的安装后，在“系统托盘”中将显示新的硬件已安装并可以使用的提示。

这样，就完成了无线网卡的安装。由于还没有可用的无线信号，所以无线网卡的状态是“不

第七章 组建无线局域网

可用的”，即带有一个红叉标记。

2. 配置双机网络

“网络连接”窗口中可以看到刚安装好的无线网卡的图标，即名称为“无线网络连接”的图标。



“无线网络连接”图标

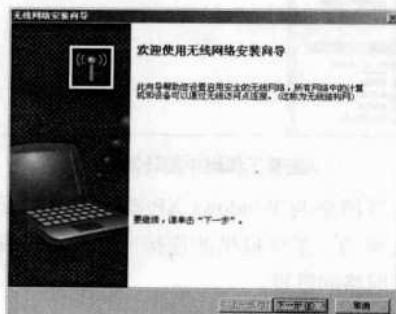
使用 Windows XP 的无线网络安装向导（SP2 版及以后版本中提供此功能），用户能够设定一个新的无线网络，或者将新设备添加到已有的无线网络中。这一切的操作将会非常容易。为此，需要执行如下操作：

STEP 1 在“控制面板”窗口中，双击如图所示的“无线网络安装向导”图标。通过运行这个向导，可以一步一步轻松完成无线网络的设置。



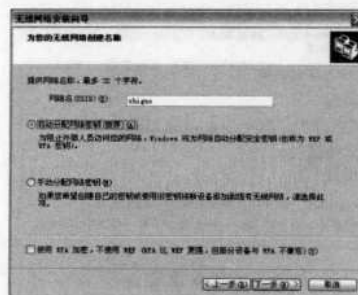
启动向导

STEP 2 出现如图所示的向导界面时，单击“下一步”按钮继续。



向导界面

STEP 3 在如图所示的“为您的无线网络创建名称”界面中，需要输入英文的网络名（SSID）。这里输入的是“zhiguo”，读者们可以自行指定。



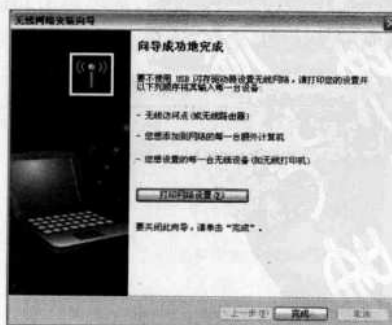
设置SSID

STEP 4 出现“您想如何设置网络？”界面时，如果网络中每一台电脑的设置方法相同，为了减少相应的网络配置工作量，可以选择使用 U 盘保存本次设置，以便在其它计算机中应用。否则，单击“手动设置网络”选项继续。



选择设置的方法

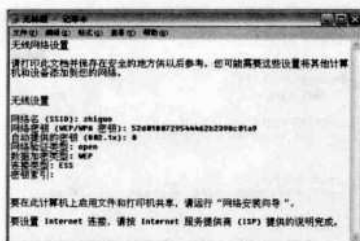
STEP 5 在出现如图所示的“向导成功完成”界面时，直接单击“完成”按钮。



完成设置



如果想查看无线向导究竟做了哪些设置，只需单击“打印网络设置”按钮，在打开的如图所示的文本文件中就可以看到详细的说明。



查看设置

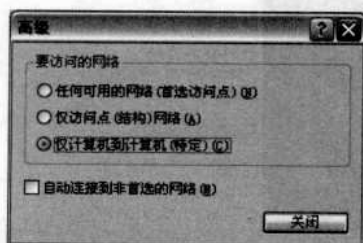
STEP 6 在“网络连接”窗口选中无线网卡图标并单击右键，在弹出的菜单中选择“属性”。

STEP 7 在弹出的“无线网络连接 属性”窗口中，单击切换到如图所示的“无线网络配置”选项卡界面，此时，可以看到多出了一个首选网络名：zhiguo。



配置属性

STEP 8 单击右下角的“高级”按钮打开如图所示的“高级”对话框。此时，需要单击勾选“仅计算机到计算机（特定）”选项。



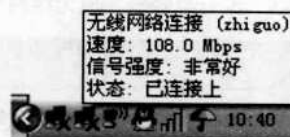
设置访问网络类型



若既直接连接至计算机，又保留连接至无线接入点（如无线路由）的功能，可选择“任何可用的网络（首选访问点）”选项。这样一来，在“首选访问点”类型的无线网络中，将会首先尝试连接到有无线接入点设备存在的无线网络。如果接入点不可用，才会继续尝试连接到对等无线网络。

稍后，在另一台电脑中也按上述方法完成无线网卡的设置，并确保两台电脑的 SSID 名称一致，即可建立起电脑之间的无线连接了。

在完成两台电脑的无线网卡设置后，在系统任务栏中可以看到无线网络连接的状态提示信息，如果出现如图所示的“无线网络连接（zhiguo）信号强度：非常好”类似的信息时，表示无线对等网络已经连接成功，



信号显示

此后，就可以在“网上邻居”对话框中通过单击左侧的“查看工作组计算机”链接，在随之切换到的如图所示对话框中，看到通过无线网卡连接起来的电脑了。



查看工作组中的计算机

无线网络与 Windows XP 操作系统的配合几乎是无缝的，系统提供的连接向导可以方便地实现无线网络的设置。

第七章 组建无线局域网

注意

由于 Windows 98/Me/2000/XP/Vista 可以自动为计算机分配 IP 地址，也就是说，即使没有为无线网卡设置 IP 地址，而且网络中没有 DHCP 服务器时，计算机也可以自动从地址段中获得一个 IP 地址，并实现彼此之间的通信，从而共享文件夹和打印机。但是，若欲实现网络的所有功能，则应当为每个网卡都分配一个 IP 地址，尤其是对小型网络而言。

7.3 使用红外线双机互联

在无线技术中，红外线数据传输也是一项常见的应用。在本节中，将讲解两台计算机之间使用红外线方式传输数据的方法，其中台式机使用红外设备是 Extended System 公司出品的 XTNDAccess IrDA PC Adapter ESI-9680。笔记本电脑使用的是 IBM 内置的红外功能 IBM ThinkPad Fast Infrared Port。

7.3.1 安装台式机红外驱动

ESI-9680 这款红外线数据传输器可以直接接在电脑的串口上，无需额外电源。在 Windows 9X/NT/XP/2003/Vista 中都自带了这款红外线数据传输器的驱动程序。这个传输器采用了标准的红外线传输协议，可以同带有红外线接口的手机、PDA、掌上电脑、笔记本电脑、台式计算机进行互传数据。最高速率可达 115,200bps，数据接收范围最高可达三米。每隔五秒钟，它就会自动搜索一下周围有没有红外线设备，找到时会自动发出声音提示，并报告找到邻近的计算机。其有效传输距离可由 0~100 公分，有效传输角度为 30 度，上下各 15 度。

在 Windows XP SP2 安装 ESI-9680 这款红外线数据传输器的驱动，需要执行如下操作：

STEP 1 将红外设备插入台式机的一个串口（com1 或 com2 任一）上。

STEP 2 依次单击“开始”→“设置”→“控

制面板”→“添加硬件”菜单，弹出如图所示的“添加硬件向导”窗口。

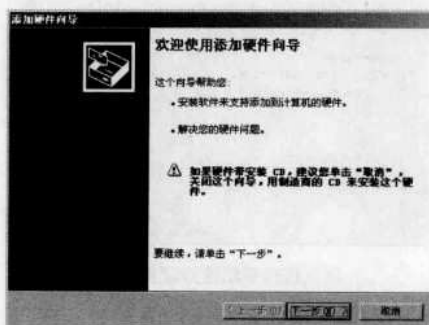


图 7-3-1 添加硬件向导

STEP 3 在出现如图所示的界面时，要选择“是，我已经连接了此硬件”项继续。

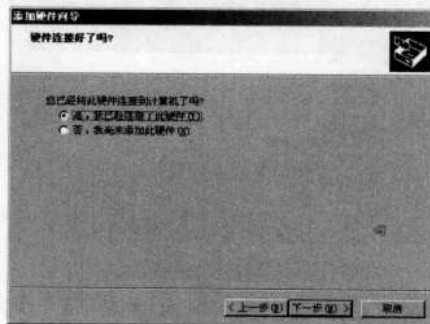


图 7-3-2 选择第一项

STEP 4 在弹出的如图所示窗口中，选择最下方的“添加新的硬件设备”项。

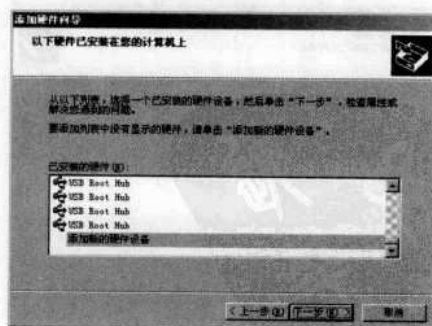
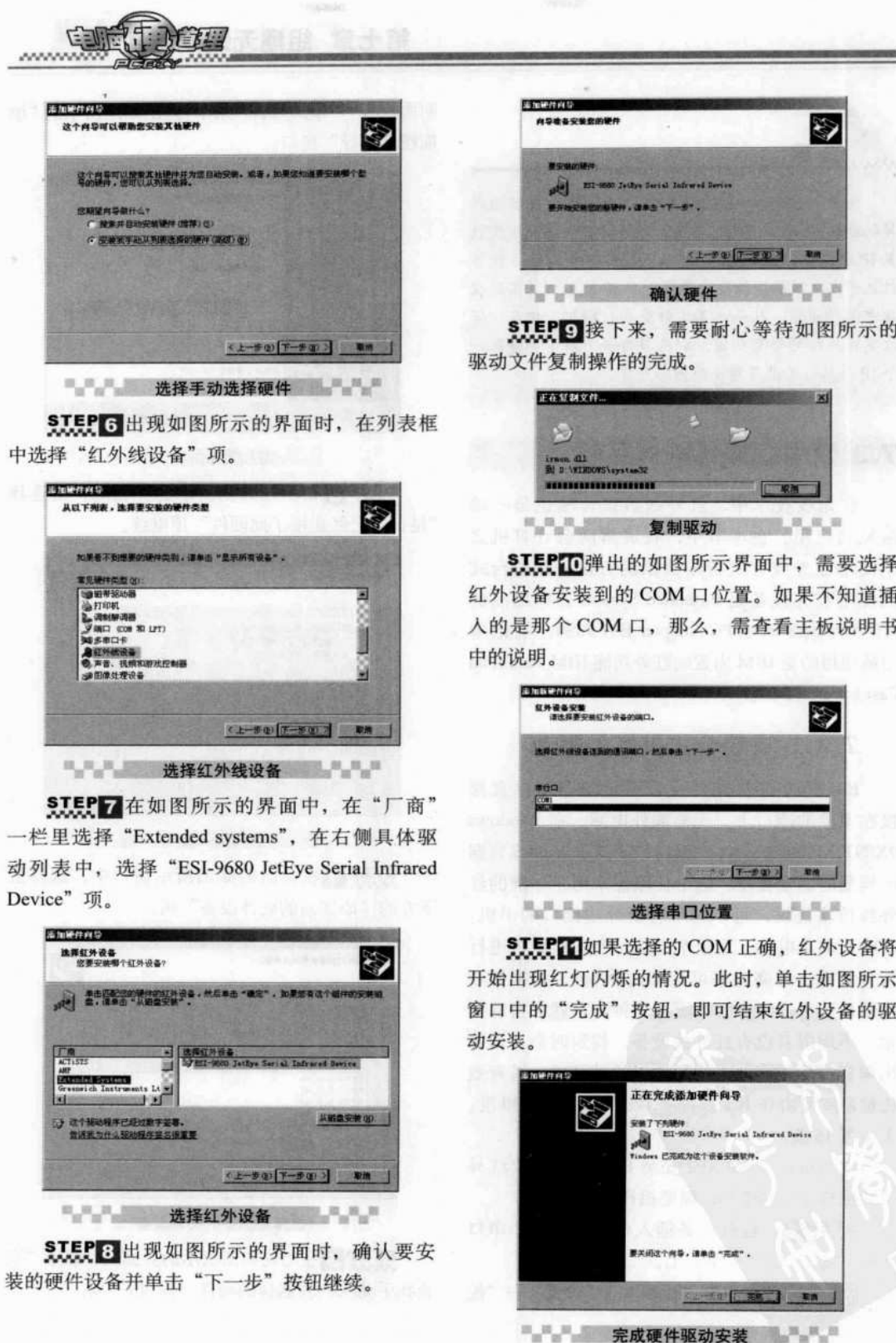


图 7-3-3 选择添加新的硬件设备

STEP 5 在出现如图所示的界面时，选择“安装我手动从列表选择的硬件（高级）”项。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



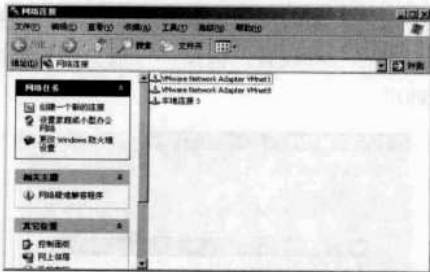
第七章 组建无线局域网

在完成驱动的安装后，在设备管理器（在运行栏中输入“Devmgmt.msc”命令可以调出设备管理器）窗口中可以看到刚刚安装完毕的红外设备。

7.3.2 设置主机

现在，需要在任意一台计算机中进行“主机”和“来宾”机的指定，这样才能进行双机的红外寻找及数据传输：

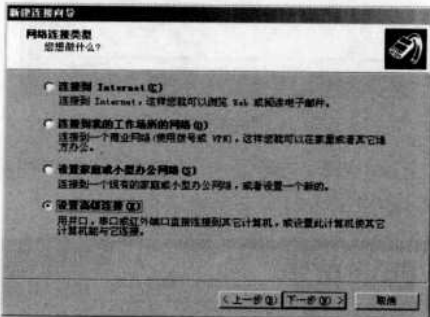
STEP 1 依次单击“开始”→“设置”→“网络连接”菜单，在弹出的如图所示窗口中，单击左侧“网络任务”列表中的“创建一个新的连接”项。



创建一个新的连接

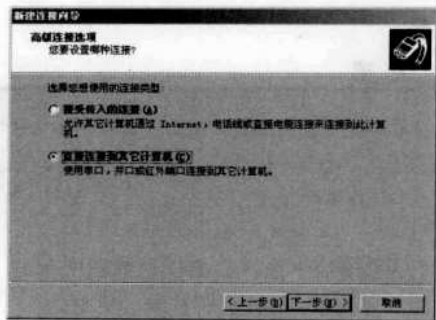
STEP 2 在弹出的“新建连接向导”窗口中单击“下一步”按钮。

STEP 3 出现如图所示的“网络连接类型”界面时，选择“设置高级连接”项继续。



选择最后一项

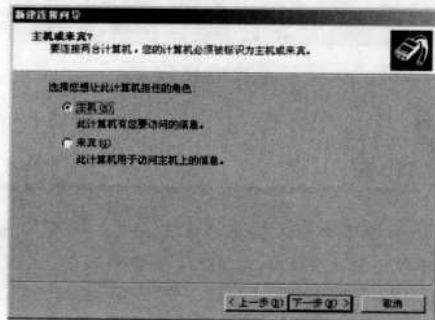
STEP 4 出现如图所示的“高级连接选项”界面时，单击选择“直接连接到其它计算机”项继续。



选择直接连接

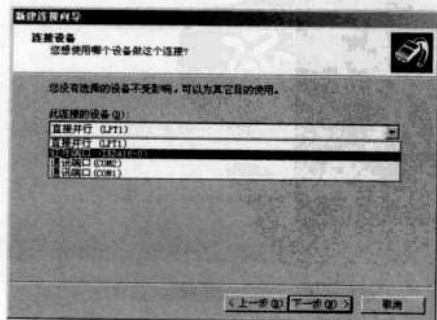
STEP 5 出现如图所示的“主机或来宾”界面中，需要根据下列情况执行某项操作：

- > 如果其它计算机访问本机的信息，单击“主机”。
- > 如果本机访问其它计算机的信息，单击“来宾”。




选择主机

STEP 6 如果指定该计算机为主机，则需要 在如图所示的界面中，在“此连接的设备”列表里选择“红外端口”。



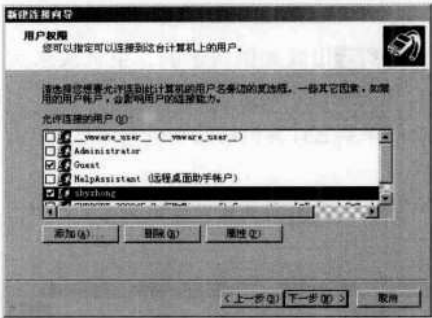
选择“红外端口”




**注意**

如果将此计算机指定为来宾，则在“连接名”中输入连接的名称。单击“下一步”后，在“选择设备”中选择“红外端口”。

STEP 7 接下来，在出现的如图所示的“用户权限”界面中，指定允许连接的用户。



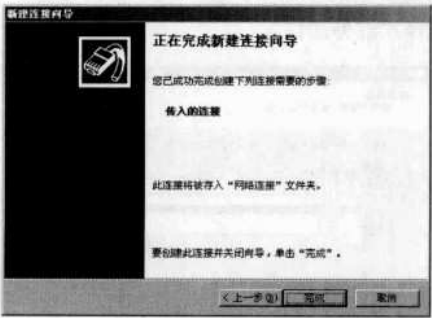
指定用户

**注意**

如果将此计算机指定为来宾，则在“可用连接”中选择“任何人使用”或“只是我使用”。

单击“下一步”。

STEP 8 当出现如图所示的界面时，单击“完成”按钮即可完成双机的红外通信设置。



完成设置

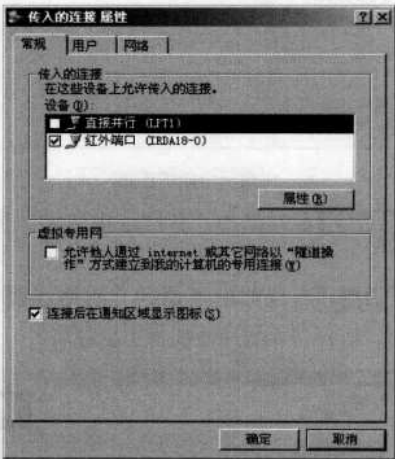
7.3.3 数据传输

完成主机的设置后，在“网络连接”窗口中将会看到如图所示的新建图标“传入的连接”。



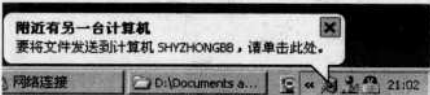
新建图标

如果进入如图所示的属性窗口，可以根据实际情况进行一些设置。但是，一般只需保持默认状态即可。



属性窗口

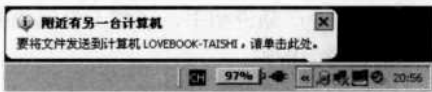
当 ESI-9680 与笔记本电脑的红外窗口相对时，将会自动弹出如图所示的提示信息。



找到另一台红外设备

与此同时，另一台计算机将自动成为“来宾”机，此计算机中会弹出类似的提示信息。

第七章 组建无线局域网



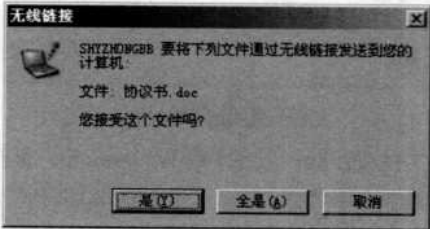
来宾机提示

此时，双击主机或来宾机系统托盘中弹出的红外设备图标，将会打开如图所示的“无线链接”窗口。



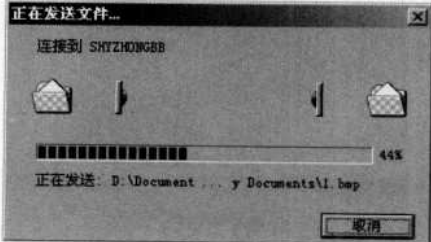
“无线链接”窗口

单击选中一个或多个文件并单击“发送”按钮后，接收数据的计算机中将会弹出如图所示的提示框。



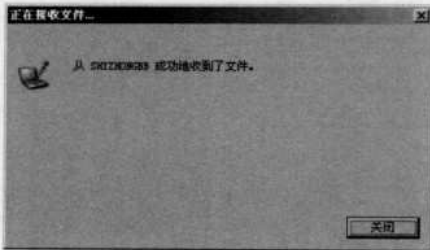
提示框

单击“是”按钮后，数据传输将会开始。在数据传输过程中，可以看到如图所示的进度框。



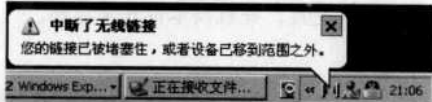
数据传输进度

完成数据传输后，接收数据的计算机中将会弹出如图所示的提示。

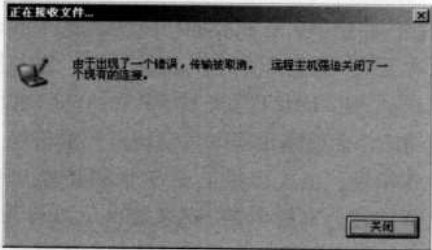


传输数据成功

传输数据时，不要将笔记本电脑的红外口或台式机的红外设备移动到红外传输角度或距离以外。也不要将手或东西放在中间，否则将会出现如图所示的提示。



如果信号被阻碍的时间较长，数据传输将会被强行中止，并弹出如图所示的提示框。



中止传输

数据传输过程中，我们可以看到系统托盘中的图标已经变成了如图所示的模样，这表示双机的数据正在交互中。



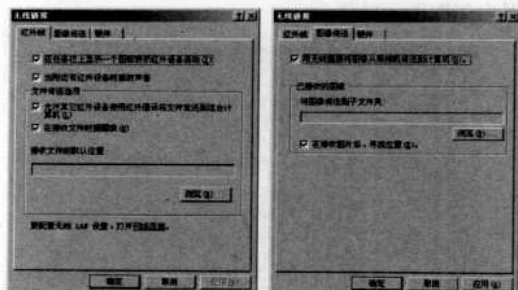
为了指定数据的接收后的存储路径，可以右键单击系统托盘中的红外图标，在弹出的快捷菜单中选择“属性”。



在接着弹出的如图所示窗口中，可以指定文



件和图像文件接收后的存储路径。



指定路径

上述就是利用红外线设备进行双机通信的过程，相对于使用无线路由与无线网卡的无线数据传输来说，使用红外设备无疑显得更为复杂和速率更慢一些。但是，红外设备也有它的优点，那就是设备非常便宜，并且技术也非常成熟。

7.4 组建无线路由局域网

无线路由（Wireless Router）就是带有无线覆盖功能的路由器，它主要的功能就是提供 Internet 接入和无线、有线（局域）网络覆盖，以及提供一些防火墙、DHCP、支持 VPN、MAC 地址过滤等功能。无线路由器既可以通过无线信号与无线设备相连，也大多提供了多个 RJ45 端口和有线设备相连。它提供的 WAN 端口可以与 ADSL MODEM 直接相连，并通过交换端口实现因特网与局域网的无缝连接。

在本节中，将讲解如何使用 D-LINK DI-624 108M 无线高速路由实现有线与无线同时存在，并能够提供 Internet 共享的混合型无线局域网。组建这种网络的操作主要分为两个部分，即：设置无线路由和设置客户端（即电脑）。

7.4.1 设置无线路由

首先，需要知道不同的无线路由使用的配置工具往往有所不同，有的使用专门的配置程序，如 Avaya，而有的则直接使用 Web 浏览器，如 D-Link。在配置无线路由之前，应当先做好以下准备工作：

❖ 146 ❖

> 认真查看产品说明书，了解无线路由默认的 IP 地址和访问密码。

> 无线路由支持自动设置客户端 IP 地址，如果希望手工设置，那么设置的 IP 地址必须与无线路由的默认 IP 地址处于同一网段。

> 将有线网卡使用 RJ45 水晶头与无线路由以太网接口连接在一起。

> 打开无线路由的电源，确认无线路由的电源指示灯和 LAN 指示灯均处于工作状态。

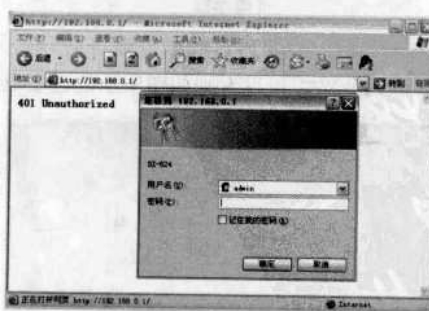
在完成上述准备工作后，接下来就可以对无线路由执行如下操作设置：

第一步，启动任意一台使用有线或无线方式连接路由的计算机，如果是使用有线方式，那么可以使用两种方式访问路由器，一是在 Vista 系统的如图所示网络窗口中，可以看到路由器的图标，双击这个图标就可以打开路由器的登录对话框。



路由器图标

二是在任意一个版本的 Windows 中，运行 IE 浏览器并在地址栏中输入“http://192.168.0.1”，按下回车键后即可打开如图所示的登录对话框。



登录对话框

第七章 组建无线局域网

1. 设置无线功能

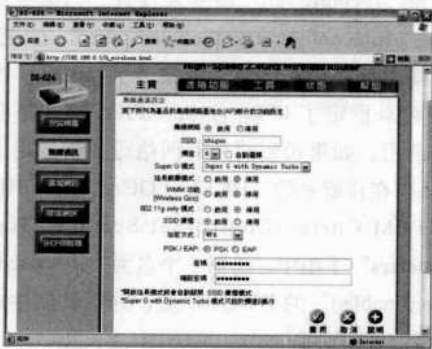
无论是使用哪种方式打开登录对话框，能够执行的操作都是一样的。下面，先来说一下如何在路由中设置无线功能。为此，需要执行如下操作：

STEP 1 在登录对话框的“用户名”中输入“admin”后，因为密码为空，所以直接单击“确定”按钮即可登录到路由器的管理界面。



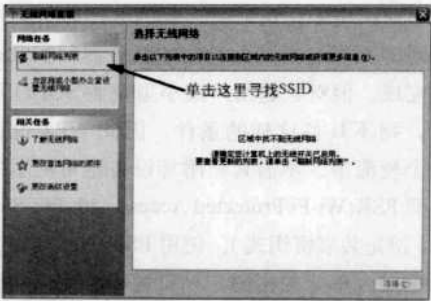
管理界面

STEP 2 在左侧单击“无线通讯”切换到如图所示的界面后，选中“无线网路”部分的“启用”项即可开始路由器的无线功能，当然默认这项功能已经是开放的。



设置无线功能

STEP 3 由于路由器出厂时默认设置的 SSID 都是一样的，所以，在 SSID 中需要输入一个自定义的 SSID 名称。SSID (Service Set Identifier) 就相当于无线网络的名称，如果有多个无线网络存在时，可以用来区分不同的网络。SSID 的名称最多可以使用 32 个字符。在无线路由将 SSID 名称广播出来后，无线网卡在使用 Windows 的扫描功能寻找到 SSID 名称后，就可以使用相应的网络信号。



Windows XP的无线扫描功能

STEP 4 为了安全起见，建议在“加密方式”列表中选择一种，这里选择了安全性较好的 WPA-PSK。选择后还需要在下方的“密码”和“确认密码”栏中输入相同的密码。这样，在无线网卡连接无线路由器时必须输入这个密码。

什么是 WPA (Wi-Fi Protected Access; Wi-Fi 保护访问)？要了解 WPA，需要先了解 WEP。WEP 的主要作用包括如下几方面：

- > 身份验证：通过密码防止未经授权用户访问网络。
- > 保证信息的保密和私有性：对数据进行加密，防止数据被窃听。
- > 保证数据的完整性：防止数据被攻击者中途恶意篡改或伪造。

由于 WEP 使用静态密钥、使用未加密循环冗余码校验 (CRC) 而无法保证加密数据完整性以及存在弱密钥等，对熟练的入侵者而言，往往只需很短时间甚至几分钟便可攻破，所以，WPA 等具有更高安全性的技术就应运而生了。从技术角度看，WPA 主要解决了 WEP 在共享密钥上的漏洞，添加了用户级的认证措施。Wi-Fi 联盟给出的 WPA 定义即为：WPA = 802.1X + EAP + TKIP + MIC。

在用户认证方面，WPA 支持两种认证协议，即 EAP 和 PSK。EAP 的全称是“Extensible Authentication Protocol”，扩展认证协议。如果选择这种认证协议，那么用户在接入无线网络前，就需要先提供相应的身份证明，通过与合法用户数据库进行比对检查，可以确认试图登录用户是否具有相应的权限。



企业网络中，认证所需要的数据库信息检索和比对的工作通常则由专门的服务器（如 Radius 来）完成。但对家庭用户或小型企业 SOHO 环境而言，则不具备这样的条件，因此 WPA 也提供了一个较简单、不需其它附加设备也可使用的模式，即 PSK(Wi-Fi Protected Access with Pre-Shared Key，预先共享密钥式)。使用 PSK 时只需在无线路由中输入单一的密码，只要客户端提供的密码相符便会获得 WLAN 的存取权限。

STEP 5 单击“套用”（即应用）按钮，即可结束此路由器无线功能配置。

2. 设置区域网路

所谓“区域网路”就是局域网，在切换到如图所示的界面后，在这里可以指定无线路由的默认 IP 地址和子网掩码地址。



设置局域网

完成这里的地址设置后，客户端的地址也会自动发生相应的变化，即自动清空 IP 地址，以便自适应路由器的设置。那么，为什么不设置 IP 地址也可以获得相应的信息呢？

这是因为在 Windows XP 中，为网络设备绑定 IP 地址有 4 种方法，即：DHCP、APIPA、手工指派和备用 IP。

其中，动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）可以实现对 TCP/IP 的自动配置。在支持 DHCP 功能的网络设备中，通常都有一个可用的 IP 地址分配范围。当一台 DHCP 客户机连到网络时，它就会自动从 DHCP 处获取一个合适的 IP 地址，从而让客户机能够正常访问网络。要将基于 Windows XP 的计算机配

置为 DHCP 客户机，只需将 IP 的获取方式设置为自动获取即可。也就是说，在“Internet 协议 (TCP/IP)”属性窗口中选中“自动获得 IP 地址”项即可。

除了 DHCP 自动分配网络参数的方法外，Windows XP 中还支持 APIPA（Automatic Private IP Addressing，自动私有 IP 地址配置）特性来分配网络参数。在 Windows XP 中，当计算机的网卡配置为“自动获得 IP 地址”，且网络环境中没有 DHCP 服务器的时候，这种方式就会起作用，此时，网卡将自动使用 169.254.0.1-169.254.255.254 这个范围内的 IP 地址，子网掩码为 255.255.255.0，并确保每台计算机的 IP 都不相同，从而实现计算机之间的互连。



注意

尽管计算机通过 APIPA 配置了 IP 地址，但是在后台，这些计算机仍然会每 5 分钟检测一次网络上的 DHCP 服务器。

要确认本机的 APIPA 特性是否被激活，可以使用“IPconfig /all”命令来检查。当命令结果中有“Autoconfiguration Enabled: Yes”的提示时，就表示当前网络连接上激活了 APIPA。当手工为网卡指定了 IP 地址时，APIPA 特性将会自动被禁用。如果希望对所有网络设置都禁用此特性，只需在注册表的“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”子项中，添加一个名为“IPAutoconfigurationEnabled”的 DWORD 值，并赋其属性内容为数字“0”即可。

当计算机处于 DHCP 或 APIPA 特性激活状态却无法进行网络操作时（如无法上网），可以先使用下面的方法进行全自动修复，一般因配置失误引起的问题都是可以轻松解决的。

STEP 1 选中“本地连接”图标并单击鼠标右键，在弹出的菜单中选择“修复”命令。

第七章 组建无线局域网



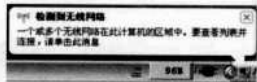
“修复”是一个很实用的功能

STEP 2 执行该命令后，将按如下顺序依次执行相应的操作：续订动态主机配置协议（DHCP）租约：ipconfig /renew；刷新地址解析协议（ARP）缓存：arp -d *；重新加载 NetBIOS 名称缓存：nbtstat -R；发送 NetBIOS 名称更新：nbtstat -RR；刷新域名系统（DNS）缓存：ipconfig /flushdns；DNS 名称注册：ipconfig /registerdns；如果你的系统是 Windows XP SP1 的话，那么还将会执行 IEEE 802.1X 身份验证重新启动操作。

STEP 3 完成了上述一系列操作后，在弹出的提示框中单击“关闭”按钮，即可结束本次的网络修复任务。

7.4.2 设置客户端

完成了无线路由的设置并重启路由后，无线信号就自动开始覆盖相应的范围了。此时，安装了无线网卡的计算机就会自动感应到信号。



感应到信号

就可以执行如下操作对客户端进行配置了：

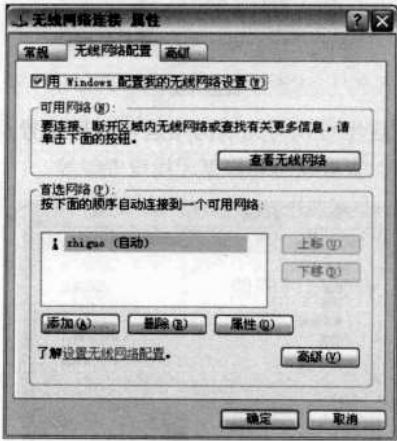
STEP 1 任一安装了无线网卡的计算机中（Windows XP SP2 环境），打开“控制面板”窗口双击“无线网络安装向导”图标。

STEP 2 在“为您的无线网络创建名称”界面中，输入无线路由中指定的 SSID 名称。

STEP 3 在“您想如何设置网络”界面中，选择“手动设置网络”项继续。

STEP 4 向导的最后一步，直接单击“完成”按钮结束设置。

STEP 5 在“网络连接”窗口中，右键单击“无线网络连接”图标并在弹出的菜单中选择“属性”，在打开的“无线网络连接 属性”对话框中单击切换到“无线网络连接”选项卡。



单击属性按钮

STEP 6 在“首选网络”列表中选择刚刚创建的“Zhiguo”网络，并单击“属性”按钮打开如图所示的对话框。



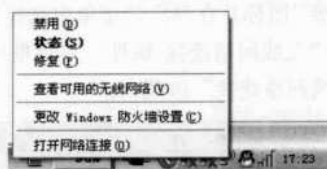
设置认证和加密信息

STEP 7 在“网络验证”列表中选择“WPA - PSK”（即在无线路由中选择项目），在“数据加密”列表中选择“TKIP”（Temporal Key Integrity Protocol，临时密钥完整性协议），并在下方的两个密钥栏中输入在无线路由中设置的密码。

单击“确定”按钮应用设置后，稍待片刻就可以在系统托盘中看到无线图标成功连接的提示



了。右键单击此图标可以看到如图所示的菜单。



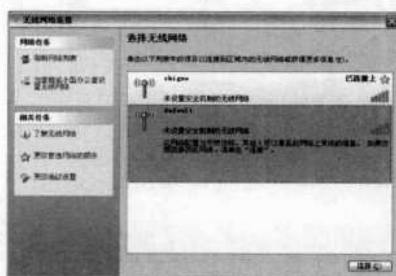
右键菜单

在这里可以对无线网络进行一些设置，如禁止使用、查看状态和修复无线设置等等。



无线状态

其中，“查看可用的无线网络”菜单可以查看当前网络中可以使用的无线网络列表，也就是有几个 SSID 名称。



无线网络列表

在这里可以看到有两个网络，也就是有两个无线路由正在广播 SSID，其中一个名称为 zhiguo，另一个名称为 default，当前正在使用的是 zhiguo 这个网络。当存在多个无线网络时，如果当前使用的网络信号比较弱，那么可以切换到另一个信号较强的网络中。

150

7.4.3 共享上网

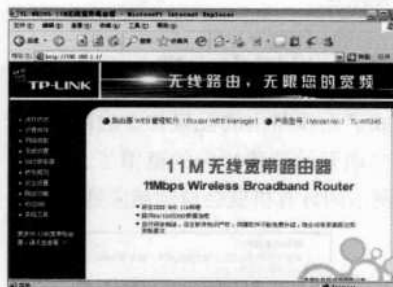
无线路由的一大魅力就是可以为局域网提供共享 Internet 的功能，要实现这项功能非常容易。以 TP-LINK 的一款无线路由为例，需要执行如下操作：

STEP 1 将 ADSL 的网线直接插入到无线路由的 WAN、DSL 等表示连接 ADSL 的端口。



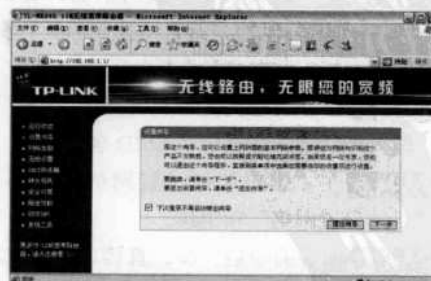
连接ADSL

STEP 2 使用无线路由说明书上提供的用户名和密码，登录到无线路由的管理界面。这个登录网址和 ADSL 的登录网址需要事先在无线路由器中设置为不同，如 ADSL 的 IP 地址为 192.168.100.100.1，无线路由的 IP 地址为 192.168.1.1，否则会有冲突。



管理界面

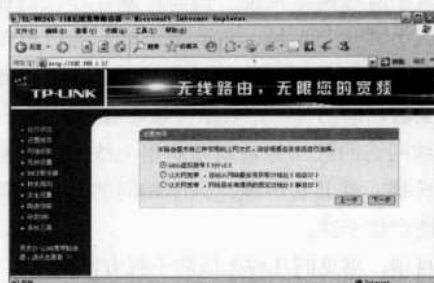
STEP 3 在左侧列表中单击“设置向导”，切换到如图所示的拨号向导界面。



拨号向导

第七章 组建无线局域网

STEP 4 单击“下一步”按钮进入如图所示的界面后，选择“ADSL 虚拟拨号”项继续。



选择拨号设置

STEP 5 出现如图所示的界面时，在“上网账号”和“上网口令”栏中输入 ISP 给的相关信息。



设置账户信息

STEP 6 出现如图所示的界面时，需要对无线网络进行基本的设置，如是否启用无线网络，以及设置 SSID 号，等。



进行无线设置

STEP 7 在出现如图所示的界面时，单击“完成”按钮即可结束共享上网设置。



完成向导设置

完成设置后，每次开启 ADSL 和无线路由的电源后，无线路由就会自动发送一个包含输入的账户信息的拨号请求给 ADSL，让 ADSL 自动与 ISP 的拨号服务器进行验证、上网。在完成上网拨号后，就可以实现局域网的共享 Internet 任务了。

7.5 无线优化措施

无线局域网的运行质量究竟如何，主要体现在无线局域网信号和传输安全两个方面。要使无线局域网运行在最佳状态，就要保证无线信号始终处于最强，而保证数据传输过程中数据的安全性，则可以防止不法之徒入侵，以免无线网络受其影响。

7.5.1 速率的优化

无线网络的传输距离、覆盖范围和穿透能力一直是人们关注的问题。无线产品的数据传输往往会受到外界和自身干扰的严重影响。所以，无线局域网产品具有共同的缺点：遇到障碍时，接收信号会急剧下降。

根据 IEEE802.11 标准，一般无线路由所能覆盖的最大距离通常为 300 米，但实际上这是个理论上的数值，无线局域网信号会随距离的增加而迅速减弱。在室外开放环境下，无线产品的传输距离最远能达到 300 米，然而在室内环境下，最远只能达到 100 米。在现实生活中，无线传输距离甚至会更短：空气、墙壁、玻璃和隔板等障碍物都会使无线信号在传输时很快衰减，再加上外界干扰、自身干扰，这些因素导致了即使在一户



家庭、一层楼房范围内，都可能存在盲区、接收不到无线信号的情况。为了解决这些问题，优化无线网络，我们可以从以下几方面着手：

1. 增加外接天线

借助于外接天线，无线的信号传输距离大幅增强。当然，这要视天线本身的增益而定。无线天线的功率单位是 dBm，dBm 表示相对于 1 毫瓦的分贝数，即：1w 是 30dBm、2w 是 33dBm、4W 是 36dBm……瓦数每增加一倍，dBm 就增加 3。为什么要用 dBm 做单位？原因大致有如下几个：

一是对于无线信号的衰减来说，不是线性的，而是成对数关系衰减的，用分贝更能体现这种关系。

二是用分贝做单位比用瓦做单位更容易描述，往往在发射机出来的功率几十上百瓦，到了接收端已经是微微瓦来计算了。

三是计算方便，衰减的计算公式用分贝来计算只用做加减法就可以了。



注意

要确保购买的天线的工作频率与无线基站的工作频率相同。如对常见的 802.11b、802.11g 产品来说，我们需要选择在 2.4 GHz 频率工作的天线。若天线放于楼顶还要选购避雷器。

2. 调整无线路由的安放位置

由于无线路由的覆盖范围是一个波形不断扩散的圆形区域，因此，无线路由应当尽量放置在无线网络的中心位置，而且各无线客户端与无线路由的直线距离最好不要超过 30 米，以避免因无线信号衰弱过多而导致的通信失败。所以在布置网络时，应该尽可能的使无线路由的位置能处于一个发射中心的位置。

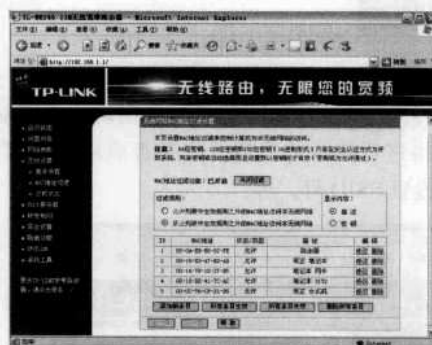
7.5.2 防干扰

对于有线网络来说，访问控制往往以物理端口接入方式进行监控，它的数据输出通过电缆传输到特定的目的地，一般情况下，只有在物理链路遭到破坏的情况下，数据传输才有可能被干扰，而无线网络的数据传输则是利用无线电波在空中辐射传播，受其它电缆、频率相同的无线设备就有可能产生干扰。

目前，常见的几种无线防干扰方法是：

一是修改 SSID。很多使用无线路由的用户都是能够实现无线信号就行，根本不对无线设备做任何调整。这样，使用同型号无线路由的用户就有“蹭网”的机会。通过修改 SSID 及启用认证方式，可以有效避免这个问题。

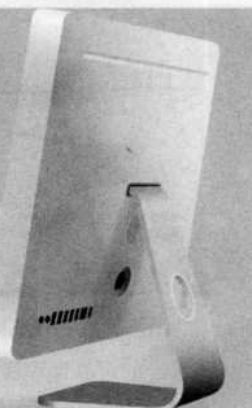
二是进行物理地址过滤。由于每个无线网卡都有惟一的物理地址，因此可以在无线路由中手工设置允许或禁止访问的权限。但由于网卡的 MAC 地址可以伪造，所以这也是较低级别的授权认证。



MAC地址过滤

三是选用端口访问控制技术。该技术也是用于无线局域网的一种增强性网络安全解决方案，当无线工作站与无线路由关联后，是否可以使用无线路由的服务要取决于 802.1x 的认证结果。

第八章 政府办公楼网络组建



从1999年开始，中国各级政府开始推行“政府上网工程”。通过组建内联全国、外联世界的计算信息网络，中国通过网络向世界展示了自己的魅力、从另外一个角度融入了世界！

从实现办公自动化、网络化办公、多功能的电子会议系统和政府应急指挥系统，到建成了对外公开的政府公众信息网站……一系列的步骤让中国政府的网络化进程令世人瞩目。

在本章中，将以组建一个中等规模的机关办公大楼网络案例为引，简要地谈一下类似机构的组网方法与要点。

8.1 系统概述与需求

时下，信息化浪起潮涌，全球各个角落无一例外地被卷入一场狂飙般的信息革命中。以高度信息化为标志的网络社会正大步朝我们走来，政府部门作为社会的重要角色，正应带头实现高度信息化，发达国家的政府机关莫不如此！

8.1.1 政府办公网络的作用

“政府上网工程”的逐步实施到位，已经改变了中国各级政府的管理模式和行政风气，大力提升了各级政府的开放性形象、提高了工作的透明度、增强了办事的效率。总的来说，政府办公网络有如下几方面的作用：

- > 实现了政府部门之间、政府与社会各界之间资讯的互通；
- > 实现了内部高效的办公自动化环境；
- > 为最终构建“电子政府”打下坚实基础；
- > 全面树立中国各级政府在世人面前的崭新形象，促进勤政和廉政建设；
- > 方便接受公众的民主监督，提高公众的参政议政意识；

> 将一些公众性资源及时发布给民众。

8.1.2 总体设计思想

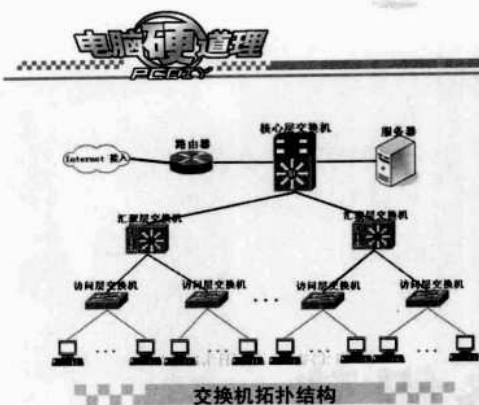
政府机关大楼的网络设计，与企事业、家庭网络的设计有较大的不同。以一个中等规模的政府机关办公大楼组建网络为例，需要把握如下几点网络设计原则：

* 系统的先进性

在设计网络时，要充分考虑到系统的先进性，尽可能地采取先进、开放的技术和产品，保证办公大楼的网络系统能够在一定时期内保持不落后。这是因为机关网络一旦运行后，就不能随意停止下来进行升级，办公大楼的网络一般会在5年左右进行一次规模不等的升级。所以，使用的网络设备要支持多协议和分级结构，这样才不会动辄就因升级而被淘汰。

* 系统的有效性和实用性

根据目前的应用及将来的发展确定网络连网手段，准确把握办公大楼网络系统要求的有效性与实用性。通过采用树型结构的网络拓扑，确保整个网络系统的分布式处理、分布处理数据库查询和分布式文件传输的速度。



*** 系统的可靠性和稳定性**

机关办公大楼网络系统作为单位高效运作的基础，其可靠性和稳定性直接关系到应用的好坏。网络系统故障可能直接给应用带来灾难性的损失。网络的可靠性主要是要防止在网络上出现因某一网点出现故障而导致全网瘫痪，如某个设备或某条线路出现故障而对整个网络系统产生影响。在维护过程中，我们得出了这样的故障大多是因为使用水晶头质量较差或是没有压好导致的。因此，网线的制作一定要严格把关。

*** 系统的安全性和保密性**

在办公大楼网络系统中，由于网络分布广、站点多，因此必须防止网络不受未授权用户的侵扰，或防止用户无意识地对网络的侵害。具体而言，必须防止如下情况：

- > 对数据的非授权修改、增删；
- > 对一些机要数据，机要文件的窃取；
- > 对网络系统的蓄意破坏；
- > 病毒的干扰；
- > 对网络环境的意外或灾难性破坏，如掉电、火灾等；

*** 网络系统的可扩展性及升级能力。**

使用高配置、高速率保证网络先进性的同时，还要注意设备应具有良好扩展性和升级能力。比方说交换机最好使用堆叠式，这样才能方便地添加计算机。其实，这一点不仅表现在网络设备上，在操作系统的选择上也要注意这一点。比方说，使用 Linux 组网的话，要花费大量的时间对机关技术人员进行培训，培训后是否能否有力完全管理网络还是个未知数。因此，建议尽量使用比较容易上手的 Windows Server 系统做服务器操作系统。

*** 维护性和管理**

机关办公大楼网络是一个较复杂的系统，其网络维护和管理十分重要，直接关系到整个网络是否能稳定而可靠地运行。除了在网络设计时要采用清晰的网络拓扑外，还应提供一整套网络测试或维护方案。另外，采用一套好的网络管理软件也是至关重要的。

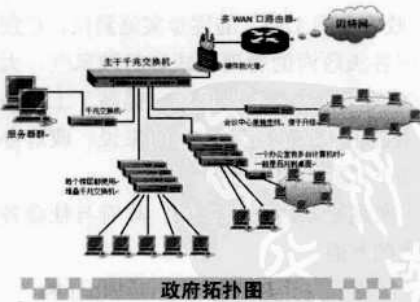
8.2 组网方案

办公局域网的最终目标是建设覆盖整个单位的互联、统一、高效、实用、安全的局域网络，近期可支持上百个，远期至少可支持上千个并发用户，提供广泛的资源共享（包括硬件、软件和信息资源的共享）。通常，在机关办公大楼的方案设计上，均会采用国际流行的分层设计，即：自顶向下进行结构化设计，自底向上实现各种业务。

本组网方案是针对某政府机关办公大楼设计的，此办公大楼楼高 9 层，整体上呈一个长方形的结构，长约 30 米，宽约 20 米，2006 年初已建成并已经在使用中，大楼共设信息点计 415 个。

8.2.1 布线设计

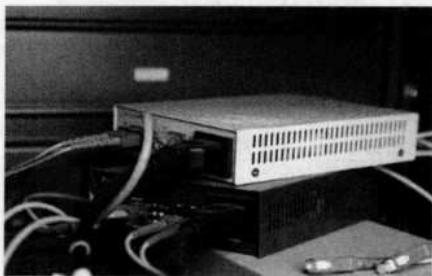
首先，要对建筑物分布、楼层层次结构、网络节点及终端进行分析。这一切最好能根据办公大楼设计图纸进行布线所需材料的计算，并从目前的网络应用实际出发，确定整个网络拓扑结构。



办公大楼的网络布线必须有较长远的考虑，虽然都是室内走线，但一般仍要求选择光纤进行主干线路架设，如各个楼层的垂直布线子系统就要使用光线进行架设。在架设光纤的过程中，光

第八章 政府办公楼网络组建

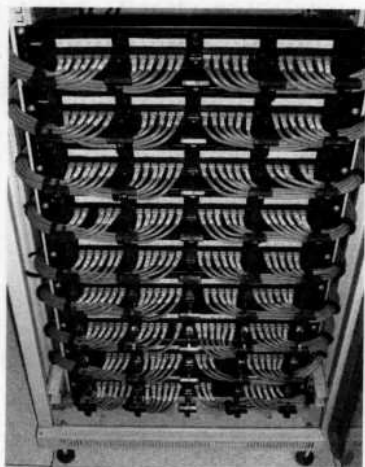
纤交换设备包括：光纤收发器、光纤耦合器、光纤交换机。在经费允许的情况下，这几样东西尽量选择品牌的。融接光纤时最好要让有经验的老师傅做，不要因为融接技术不过关为今后的网络调试、运行留下隐患。



光纤

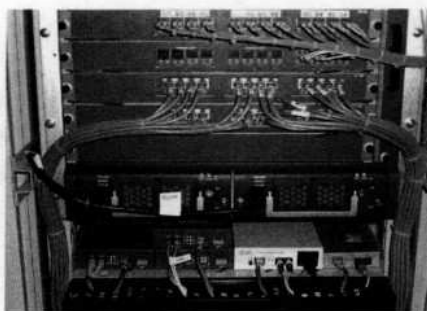
对于连接同一楼层各个房间入网计算机的水平布线子系统，一般使用五类或超五类双绞线。

局域网布线时，应该充分考虑到将来网络扩展可能需要的最大接入节点数量、接入位置的分布和用户使用的方便性。若整座建筑物接入局域网的节点计算机不多，可以采用从一个接入层节点直接连接所有楼层入网节点的设计。



机房直接到桌面

若建筑物的每个楼层都分布有大量接入节点，就需要设计垂直布线子系统和水平布线子系统，并且在每层楼设置专门的配线间，用于安置该楼层的访问层节点网络设备和配线装置。



分层布线

规模较大的单位一般都配有中心机房，考虑到网络中心机房在整个网络中所处的核心位置，为了保持其长时间运行的可靠性，建议对机房采取以下必要的措施：

- * 防尘、防静电、安装数据地线

对机房铺设防静电地板及安装必要的通风和温度调节设备，建议最好安装单独的数据地线。

- * 电源保护

由于市电供应的电压不稳定产生的浪涌及断电，将对各种电脑和网络设备造成不可预知的伤害，所以应在中心机房加设稳压装置，网络中心机房最好采用一台 UPS，容量的大小根据网络规模与设备多少而定。



UPS不间断电源

比较理想的电路设计就是安装双线路，这样当一条线路出现停电等问题时，另一条线路就可以立即供应电力，配合 UPS 保证中心机房稳定过渡这个非常瞬间。

- * 防雷

由于中心机房内摆放了大量贵重的电子设备，所以，雷雨季节应特别注意防雷。雷电的防护可



分为直击雷和感应雷的防护两方面。

*** 恒温**

中心机房的恒温问题是很关键的，光依靠办公大楼中的中央空调是不起什么作用的。当然有总比没有强，通常中心机房会放一台 5 匹的柜机进行温度控制。

8.2.2 网络设备

为保证办公大楼网络系统的稳定性和高效运行，经费不紧张的前提下，尽量采用主流的品牌网络产品，推荐使用思科（CISCO）、华为（HUAWEI）、北电（NORTEL）、锐捷（REDGIANT）、3COM、IBM、H3C 等产品。这些公司的产品虽然性价比不高，但产品的质量和技术都是业界一流的。比方说，思科公司提供了业界范围最广的网络硬件产品、互联网操作系统（IOS）软件、网络设计和实施等专业技术支持，并与合作伙伴合作提供网络维护、优化等方面的技术支持和专业化培训服务。

1. 核心层设计

网络核心层是网络的中心，用于实现高性能的交换和传输。因此核心层设备应该是高性能的交换设备，具有高速、非常可靠、不间断工作等特性。路由器的选择上，推荐使用 Cisco 公司的路由器，因为该公司的路由器已经相当于业界默认的标准，并且 Cisco 路由器的高性能在业界中也是首屈一指的。前几年和至今的一些办公大楼中，网络骨干设备都是选用 Cisco 7206VXR 这样的路由器作为核心交换设备来连接各级交换机。



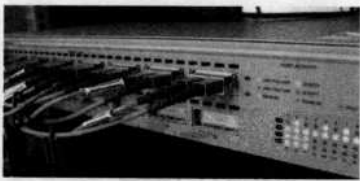
核心路由器

如果经费比较紧张，也可以使用 H3C RT-

MSR5060-AC-H3 这样的路由器。路由器需要放置在办公大楼的中心主机房内。以 H3C RT-MSR5060-AC-H3 为例，它具有 2 个千兆光纤端口、16 个插槽，具备了完善的管理功能。基本的规格如下表所示。

H3C RT-MSR5060-AC-H3基本规格	
路由器类型	企业级路由器
路由器处理器	RISC新一代处理器(833MHz)
最大Flash内存	1024MB
最大DRAM内存	1024MB
局域网接口	2个千兆光/电
扩展插槽	16个
路由器包转发率	600KPPS
路由器网络协议	IP服务,非IP服务,IP应用,IP路由,MPLS,IPv6,广域网协议,局域网协议
路由器网管功能	网络管理,本地管理,用户接入管理
VPN功能	支持VPN
防火墙功能	内置
安全标准	UL 60950 3rd Edition, CSA 22.2#950 3rd Edition 1995, EN 60950: 2000 + ZB & ZC deviations for European Union LVD Directive, IEC 60950:1999 + corr. Feb. 2000, modified + all National deviations
机身重量	20kg
外观尺寸	436.2 × 424 × 175.1mm

在核心层交换机的选用上，可以使用具有全光纤接口的设备。这样的设备有很多，如 TP-LINK TL-SF2808C 全光纤智能以太网交换机等等。这样的交换机可以实现高速办公网与高速 Internet 的无缝连接。



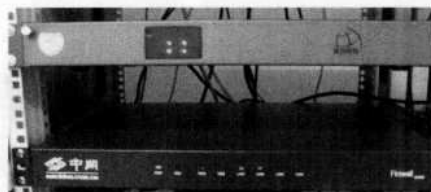
全光纤智能以太网交换机

以 TL-SF2808C 这款交换机为例，它提供了 8 个 100Mbps 光纤端口，最大传输距离可达 2km。在距离上完全可以满足办公大楼的布线需求。因为具有全中文的配置环境，所以技术人员稍加培训就可以通过软件配置此产品。由于办公大楼中信息点较多，容易产生广播风暴，所以主干交换机的选择一定具有强大的广播风暴控制能力，

第八章 政府办公楼网络组建

可以有效减少广播风暴或分割广播风暴。

在机房中网络安全设备是必不可少的，安全设备不仅仅只是硬件防火墙，防火墙只是一个整个安全体系中的重要组成部分。如图所示的是2个千兆硬件防火墙设备。



硬件防火墙

现在比较流行的、仍然具有可观效果的攻击还数 DDoS，这种依靠发送大量小而多数据进行攻击的方法，无论是软件防火墙还是硬件防火墙，只要遭遇了就可能产生很大的负面效果。所以，即使是配备了硬件级的防火墙也不能掉以轻心，因为有时遇到海浪式的攻击时，硬件防火墙也会很快招架不住的，只有网络管理人员时刻保持高度的责任心，才能保证网络在遭受攻击时快速解决问题。

对于重要的政府机关来说，安全过滤网关也是不可或缺的。通过这个设备可以有效过滤病毒、敏感字符、垃圾邮件等等。



电子邮件安全网关

只要是数据经过安全过滤网关，那么，客户机计算机的一切网络交换情况就可以了如指掌。比方说访问过的网站、在论坛上发的消息、使用的 IP 地址……都可以进行监控的。对于企业、学校来说，这样的设备不常见，但是在一些重要的政府机关里，这样的设备在组网时必须考虑在内。

2. 汇聚层/接入层

汇聚层主要负责连接访问层和核心层，通过汇集分散的访问点，可以扩大核心层设备的端口密度和种类，通过汇聚各区域的数据流量，可以实现骨干网络之间的传输优化。此外，汇聚层交

换机还负责本区域内的数据交换，汇聚交换机一般与核心交换机同类型，仍需要较高的性能和比较丰富的功能，但吞吐量较低。

接入层网络作为二层交换网络，提供工作站等设备的网络接入。接入层的交换机在整个网络中的数量最多，它具有即插即用的特性。对此类交换机的要求，一是价格合理；二是可管理性好，易于使用和维护；三是有足够的吞吐量；四是稳定性好，能够在比较恶劣的环境下稳定地工作。

由于 415 个信息点平均分布在 9 层办公大楼中，每层只有 46 个端口需求，考虑到相当一部分的信息端口基本不用，所以，可以将汇聚层与接入层合并，即直接在每个楼层配置堆叠交换机与计算机直接相连。



堆叠交换机

本方案选用了 D_LINK DES-3526/3550 2 层可堆叠交换机，这个系列的可堆叠交换机具有 24/48 个 10/100BASE-TX 端口和 2 个组合式 1000BASE-T/SFP 千兆端口，这样的设计可以提供更加安全及灵活的连接方式。DES-35xx 系列交换机操作简便，易于管理。通过此交换机可以构建具有灵活的千兆上行链路及 10/100Mbps 速率的部门级网络。堆叠单元之间的数据量的传输通过快速全双工模式千兆接口和网络电缆来完成。此外，网管还可以轻松添加至每堆叠单元 32 个交换机。

DES-35xx 系列交换机在连接和存取控制上提供了一套完整的安全保障措施。包含了基于 MAC 地址的访问控制列表 (ACLs)、交换机端口表、IP 地址表、TCP/UDP 端口号、802.1x 网络访问控制协议的用户授权和 MAC 地址控制等措施。DES-35xx 系列还提供了 TACACS + RADIUS 进行集中管理。通过和网络应用控制的集成，这套安全保障措施不仅能保证用户的正常访问，而且还能阻断恶意的大流量在网络中传播。

DES-35xx 系列交换机能简化并加速管理任



务，通过内置的 Web 管理，网管能从树型结构报表了解每个堆叠单元的详细信息，从网络拓扑图中了解堆叠单元的位置以及他们链接信息。这种简单而有效的基于 Web 的管理，能够节省安装昂贵的基于简单网络管理协议（SNMP）的网络管理软件的费用。

有的房间可能会有多台电脑，对于这样的房间就要从墙壁上的信息插座引出一根网线到百兆交换机上，实现百兆到桌面即可。

3. 服务器

在机关大楼的中心机房中，服务器也是一个重要的网络设备。通过服务器可以对内提供高性能、高容量的数据存储服务，对外可以提供高速、稳定的公众服务。在本设计方案中共选用了两台服务器，一台是对内提供数据存储、视频点播等服务的 IBM System x3400 系列服务器。



IBM System x3400

IBM 服务器在业内具备相当好的口碑，这款 IBM System X3400 (7976I15) 就是其中一款比较经典的服务器产品，它配备了英特尔至强四核 E5420 处理器，主频为 2GHz，拥有 12MB 二级缓存，最多可扩展至 2 路处理器。在磁盘存储方面提供了串行硬盘支持，这样单位可以根据数据存储量的不断倍增而适当进行硬盘升级。如今的硬盘价格是越来越便宜，所以用户自行配置硬盘的话，可以节省很多资金。在内存方面，服务器标配了 2GB 内存，最大内存容量可扩展至 32GB。在网络方面，服务器集成了千兆以太网适配器，采用了塔式设计结构，并且提供 3 年有限现场保修服务。此服务器的基本参数见如下表所示。

❖ 158 ❖

对外服务器方面，选择 IBM System x3650 7979R01 服务器。网络方面提供 2 个光纤接口处理因特网的数据。硬盘方面标配 146GB 硬盘，满足一般性机关业务处理，如果存储容量不够也可扩充。另外，还配备光路诊断系统，是 IBM 服务器产品的一个非常有特色的、非常实用的功能。



IBM System x3650



光路诊断系统

IBM 的服务器上，故障的发现、诊断可以被分为三个阶段。第一个阶段是从前面板的信息指示灯来大致判断服务器是否工作正常，如果有故障则进一步查询光路诊断面板可以进一步缩小故障的范围，如果有必要的话，用户可以打开机箱盖查看服务器内部，在主板上，几乎每一个主要的配件盘片还有设计有相应的指示灯，比如 CPU 指示灯、VRM 指示灯、电池指示灯、DIMMM 指示灯等。

8.2.3 子网划分

在一个大、中型网络里，VLAN 的划分是必不可少的一步骤之一。在本办公网设计方案中，整个办公中的 VLAN 及 IP 编址方案如下表所示。

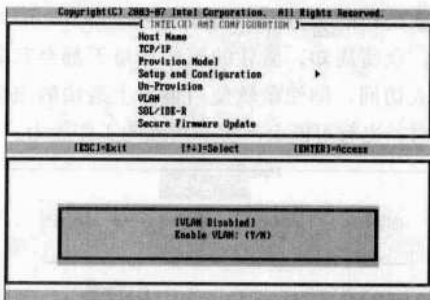
VLAN号	VLAN名称	IP网段	默认网关	说明
VLAN1	任意起	192.168.0.0/24	192.168.0.254	一楼
VLAN10	任意起	192.168.1.0/24	192.168.1.254	二楼
VLAN20	任意起	192.168.2.0/24	192.168.2.254	三楼

第八章 政府办公楼网络组建

VLAN30	任意起	192.168.3.0/24	192.168.3.254	四楼
VLAN40	任意起	192.168.4.0/24	192.168.4.254	五楼
VLAN50	任意起	192.168.5.0/24	192.168.5.254	六楼
VLAN60	任意起	192.168.6.0/24	192.168.6.254	七楼
VLAN70	任意起	192.168.7.0/24	192.168.7.254	八楼
VLAN80	任意起	192.168.8.0/24	192.168.8.254	九楼

为了简化起见，这里只规划了九个VLAN，同时推荐为每个VLAN定义了一个由拼音缩写组成的VLAN名称，方便后继技术人员管理时识别。

本设计方案使用的交换机都提供了划分VLAN（虚拟局域网）的功能，使网络管理员可以根据需要将用户划分为几个不同的组。这样既便于管理，又可以提高安全性。虚拟局域网不受设备物理位置的限制，灵活性较大。



VLAN管理功能

VLAN实现通常是以端口为中心的，与节点相连的端口将确定它所驻留的VLAN。将端口分配给VLAN的方式有两种，分别是静态的和动态的，形成静态VLAN的过程是将端口强制性地分配给VLAN的过程。即我们先在VTP（VLAN Trunking Protocol）Server上建立VLAN，然后将每个端口分配给相应的VLAN的过程。这是我们创建VLAN最常用的方法。

动态VLAN形成很简单，由端口决定自己属于哪个VLAN。即我们先建立一个VMPS（VLAN Membership Policy Server）VLAN管理策略服务器，里面包含一个文本文件，文件中存有与VLAN映射的MAC地址表。交换机根据映射表决定将端口分配给何种VLAN。这种方法有很大优势，但是创建数据库是一项非常艰苦而且非常繁琐的工作。

配置VLAN需要在交换设备中进行，交换机、路由器一样通常有以下几种管理配置方式：

> 通过Console端口连接到设备，使用命令行配置；

> 使用Telnet登录到设备；

> 使用Web方式登录到设备；

> 使用电话及modem远程配置；

> 使用SSH安全登录到设备；

> NMS（Network Management Station）使用SNMP（Simple Network Management Protocol，简单网络管理协议）或RMON（Remote Monitor）。

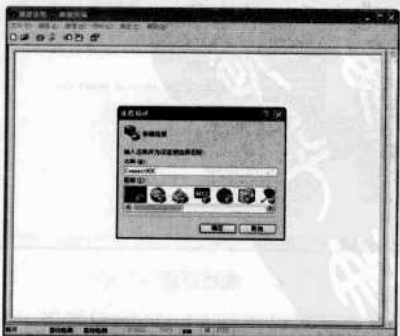
以上几种方式中，使用Console端口是最基本的方式。通常，初次配置必需使用Console端口与计算机的COM端口相连，使用Windows的超级终端程序登录到交换机。为此，需执行如下操作：

STEP 1 用附带的Console线缆连接交换设备的Console端口和计算机的COM端口。为交换设备通电启动，运行Windows XP中的超级终端。



超级终端

STEP 2 在弹出的如图所示对话框中，输入一个新的连接名称。



新建连接



STEP 3 在弹出的“连接到”对话框中，选择连接到串口位置并单击“确定”按钮。



选择串口

STEP 4 在弹出的 COMX 属性对话框中，将“每秒位数”设置为 9600，其余选择默认值并单击“确定”按钮。



COMX属性对话框

STEP 5 很快就会出现如图所示的提示信息，并进入交换设备的操作状态。



成功登录

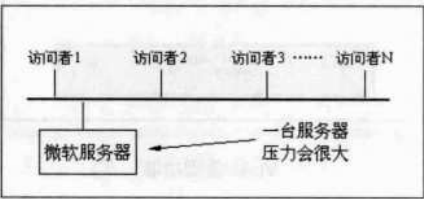
现在，就可以进行 VLAN 的配置了，具体的操作请见交换设备的说明书，此处略。

8.3 群集在服务器中的应用

政府大量通过网络化向公众提服务时，有些机关服务器的压力很大。这时，使用群集服务是减轻服务器工作压力的最实用的设计之一，它可以有效保证服务器不会因访问量过大而出现速度缓慢、死机等现象，同时亦可以确保浏览者能够最快、最稳定地访问服务器。那么，群集服务究竟是怎么回事？如何与各种服务器之前进行合作？下面，就让我们一起来探讨群集的魅力！

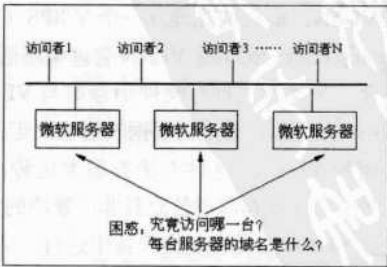
8.3.1 什么是群集服务

什么是群集服务呢？下面让我们举例说明。以微软公司的服务器“http://www.microsoft.com”为例，众所周知，微软的服务器每天都有非常多的人访问，即使微软使用世界上最快的服务器来应对，也有可能产生非常强的工作压力。



一台服务器的压力很大

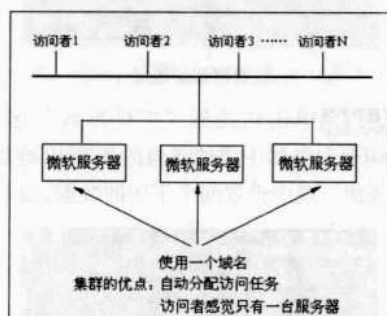
这个时候，解决的方法通常是添加服务器。但这样做，就会产生很多问题，比方说：每台服务器的域名是什么？按照常规的设计方法，就是第一台服务器是“www.microsoft.com”；第二台服务器是“www.1.microsoft.com”；第三台服务器就是“www.2.microsoft.com”。但是，如此多的域名怎样才能让访问者记住？



多台服务器

第八章 政府办公楼网络组建

显然，这不仅会造成域名资源的浪费和费用的支出，更增加了域名维护的工作量。更重要的是，会给访问者带来很多访问上的麻烦。因此，我们就需要一个解决的方法，这个解决的方法就是“群集”（Cluster）服务。群集服务器可以允许最多添加 32 台服务器，这些服务器统统使用一个域名，当一台服务器忙不过来时，会自动将访问压力“释放”到其它不忙碌的服务器中。



集群服务示意

这样一来，对于访问者来说，能享受到的最大好处就是：不必再去记哪台服务器是使用哪个域名了，他们会认为“微软就是一台服务器在提供服务”。对于服务器来说，一则可以减轻域名的维护压力；二则可以减轻服务器本身的工作压力。这不仅会使服务器能够保证访问者的浏览服务正常，还能在一定程度上使服务器的寿命得到延长。

根据群集服务的工作特点，我们可以看出该服务其实起到的就是一种“负载均衡”的效果，它可以有效地完善服务器的管理能力，以及减轻和分发访问压力。显然，这是一种极为实用的服务器管理技术。按照标准的称呼，我们应将这种技术称之为“网络负载均衡群集”（Network Load Balancing Clusters, NLBC）。这项技术最早出现在 Windows 2000 Server 的 Advanced Server（高级服务器）系统中，在 Windows Server 2003 的各种版本中，微软均提供了这项功能。

但是，群集的使用也是要注意应用环境的，比方说 Web 服务器、终端服务器就可以很好地应用群集，但是某些交互式的应用程序服务器则可能不适合群集。例如，我们使用了两台 Web 服

器构成了群集，这两台服务器的任务就是接受用户的某些订单，如果这些订单数据都是保存在本地数据库中，那么这将会形成两个数据内容截然不同的数据库，此时就必须将这些数据合并起来，但这样做起来就会很累，但我们却必须这样做，否则，我们将会看到以下这种糟糕的情况：用户如果第一次是在第一台服务器中建立了订单，第二次访问被分配到第二台服务器后，他将查不到第一次下的订单！

当然，这种糟糕的情况，我们也可以通过共享一台专门用于数据存储的服务器来解决。但是，这又添加了一台额外服务器的支出与维护。因此，群集的使用就值得考虑了。所以在没有完善的条件和规划下，有些环境的确不推荐使用群集服务。

8.3.2 建立群集实战

使用群集功能，并不是单击一下鼠标或是按下 Enter 键这么简单。这项功能的启用需要服务器必须符合一些条件才能正常使用。下面，让我们以两台服务器建立群集服务为例，看看都需要哪些条件：

- > 每台服务器都需要有一个静态的 IP 地址；
- > 需要另外准备一个静态 IP 地址，作为共享的群集地址；
- > 需要每台服务器安装 IIS（Internet Information Service, IIS）组件；
- > 需要所有服务器有相同的内容。

在明白了上述这些最基本的组件条件后，下面让我们来了解一下两台服务器的基本情况：第一服务器名为 zhong，静态地址为 192.168.1.2；第二台服务器名为 zhong1，静态地址为 192.168.1.3。群集共享的 IP 地址为 192.168.1.6。

现在，需要对两台服务器进行静态 IP 地址的配置。这个操作非常简单，所以，下面只说第一台服务器的设置过程，第二台服务器的设置方法只需跟着照做就可以了。

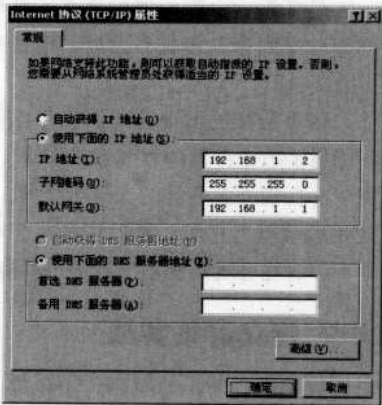
STEP 1 在第一台服务器中依次单击“开始”→“设置”→“网络连接”菜单，在打开的窗口中选中网卡（即“本地连接”图标）并单击鼠标右键，接着在弹出的快捷菜单中选择“属性”命令。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



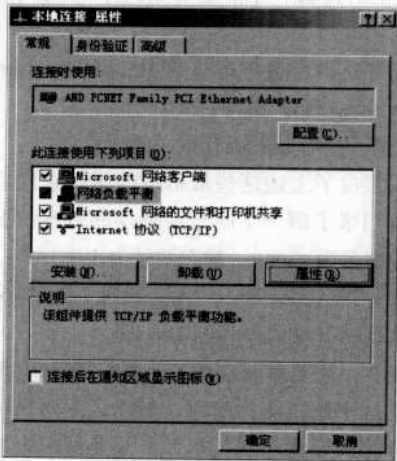
STEP 2 在“本地连接 属性”窗口中，选中“TCP/IP 协议 (TCP/IP)”项并单击“属性”按钮。

STEP 3 在“TCP/IP 协议 (TCP/IP)”属性设置界面中，添加静态 IP 地址 192.168.1.2。接着，按第一台服务器的设置方法，为第二台服务器添加好静态 IP 地址。



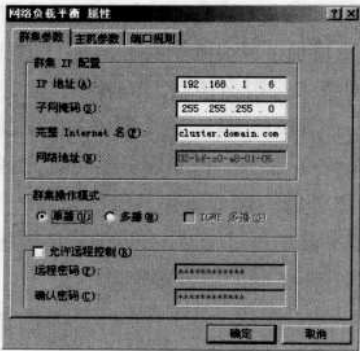
设置服务器IP地址

STEP 4 现在需要配置群集 IP 地址。分别进入 A 和 B 两台计算机的“本地连接”属性界面，勾选“此连接使用下列项目”中的“网络负载平衡”项并单击其“属性”按钮。



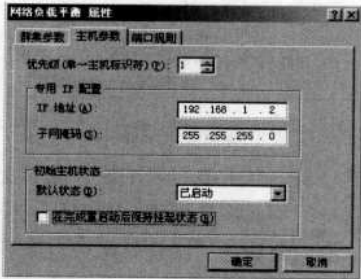
启用负载平衡

STEP 5 在“网络负载平衡 属性”对话框中，分别为两台服务器添加 192.168.1.6 这个群集 IP 地址，并将子网掩码设置为 255.255.255.0。



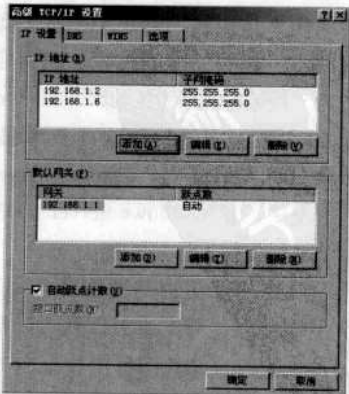
设置群集IP地址

STEP 6 单击切换到“主机参数”选项卡，分别在两台服务器中添加各自的静态 IP 地址，并在“优先级”项中设置两个不同的数据，如 1 和 2。



设置数据

STEP 7 分别在两台服务器的“TCP/IP 协议 (TCP/IP)”属性设置界面中，单击“高级”按钮并弹出的“高级 TCP/IP 设置”界面中，单击“添加”按钮添加群集 IP 地址 192.100.100.6 和子网掩码 255.255.255.0。



添加IP地址

第八章 政府办公楼网络组建

STEP 3 退出两台计算机的“本地连接”属性窗口，并耐心等待 5~8 分钟让系统完成设置。在设置完毕后，可以先将两台服务器 IIS 中的网站首页内容稍做修改，比方说分别加一个记号。然后，使用局域网中的多台计算机，在打开的 IE 窗口中请直接使用 192.168.1.6 这个群集 IP 地址进行访问，如果出现以下状态则都是正常的。

> 有的计算机出现第一台服务器的网站首页内容（记号），有的计算机出现第二台服务器的网站首页内容（记号），这表示群集的 IP 是可以访问到两台服务器内容的。

> 两台都出现某台服务器的网站首页内容，这也正是群集想要达到的效果。

注意

不要试图从一台群集服务器中使用 Ping 命令来测试另一台群集服务器。因为 NLB 带来的一个负面效应，就是虽然所有的群集成员都可以同样方便地连接到客户端，但是群集成员之间是不能通信的。

8.4 架设SSL网站

默认情况下，IIS 使用 HTTP 协议以明文形式传输数据，没有采取任何加密措施，用户的重要数据很容易被窃取。显然有些政府网站中的数据是需要进行保护的，有经验的网管就会在这个时候使用 SSL 技术来增强 IIS 服务器的通信安全。

SSL (Security Socket Layer) 全称是加密套接字协议层，它位于 HTTP 协议层和 TGP 协议层之间，用于建立用户与服务器之间的加密通信，确保所传递信息的安全性，同时 SSL 安全机制是依靠数字证书来实现的。SSL 基于公用密钥和私人密钥，用户使用公用密钥来加密数据，但解密数据必须要使用相应的私人密钥。

使用 SSL 安全机制的通信过程如下：用户与 IIS 服务器建立连接后，服务器会把数字证书与公用密钥发送给用户，用户端生成会话密钥，并用公共密钥对会话密钥进行加密，然后传递给服务器，服务器端用私人密钥进行解密，这样，用户

端和服务器端就建立了一条安全通道，只有 SSL 允许的用户才能与 IIS 服务器进行通信。

注意

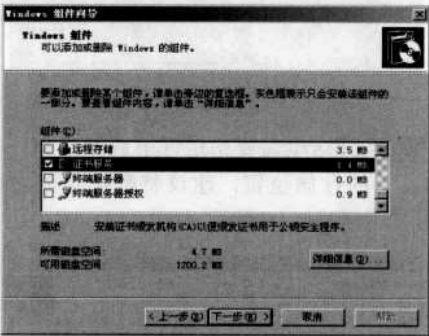
SSL 网站不同于一般的 Web 站点，使用的是“HTTPS”协议，而不是普通的“HTTP”协议。因此 URL(统一资源定位器) 格式为 https:// 网站域名。

8.4.1 安装证书服务

要使用 SSL 安全机制功能，必须先为 Windows Server 2003 系统安装证书服务：

STEP 1 依次单击“开始”→“设置”→“控制面板”→“添加或删除程序”，在弹出的窗口中单击左侧导航栏中的“添加 / 删除 Windows 组件”项进入“Windows 组件向导”对话框。

STEP 2 拖动右侧的滚动条至最下方，在出现“证书服务”项后使用鼠标单击选中它。



选择要安装的组件

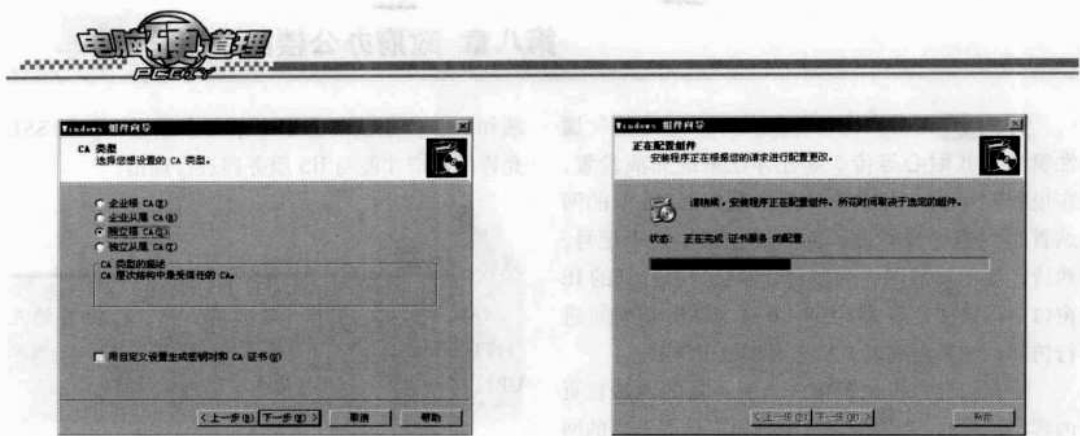
STEP 3 在随即弹出的提示框中，单击“是”按钮确认选中操作。



单击“是”按钮

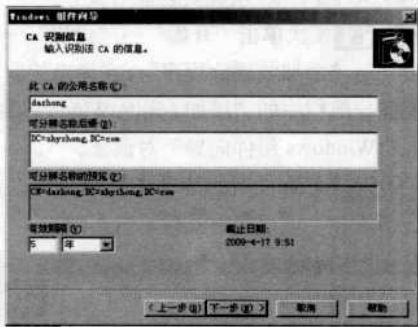
STEP 4 在出现的“CA 类型”对话框中，选择“独立根 CA”项后继续。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



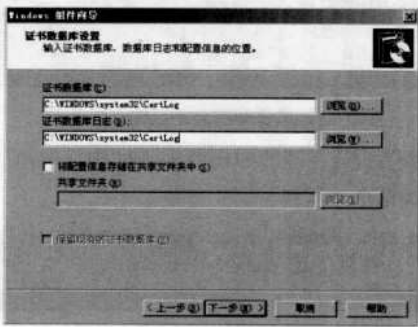
选择“独立根CA”项

STEP 5 在下一步中需要为 CA 服务器取个名字（如 dazhong），及设置证书的有效期限。



取个名字

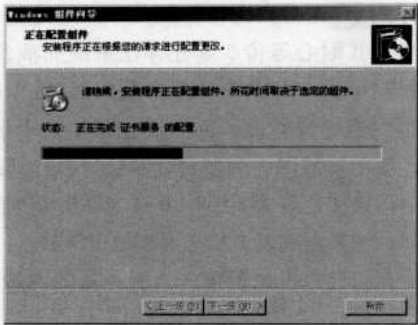
STEP 6 这里需要指定证书数据库和证书数据库日志的存储位置，建议将数据存储在 NTFS 文件系统的分区中。



设置路径

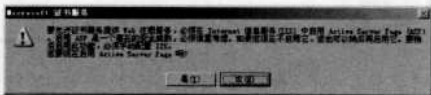
STEP 7 在弹出的提示框中单击“是”按钮继续。

STEP 8 稍后系统将开始从 Windows Server 2003 安装光盘复制文件到当前系统。



复制文件

如果当前 IIS 中没有启动 ASP 的支持，那么复制文件的过程中，将会弹出一个提示框，告之必须启用 Active Server Page (ASP)，此时单击“是”按钮继续，即可完成“证书服务”组件的安装。



单击“是”按钮

8.4.2 配置SSL网站

完成了证书服务的安装后，就可以为要使用 SSL 安全机制的网站创建请求证书文件。为此，需要执行如下操作：

STEP 9 依次单击“开始”→“设置”→“控制面板”→“管理工具”→“Internet 信息服务 (IIS) 管理器”菜单项，在弹出的管理器窗口中单击展开“网站”目录，右键选中并单击打算使用 SSL 的网站（如 shyzhong001），在弹出的快捷菜单中选择“属性”。



选择属性

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

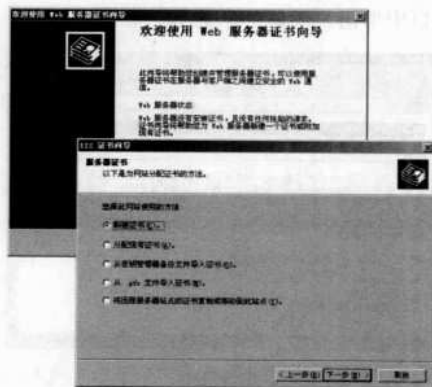
第八章 政府办公楼网络组建

STEP10在打开的“shyzhong001 属性”对话框中单击切换到“目录安全性”选项卡设置界面，然后单击“服务器证书”按钮。



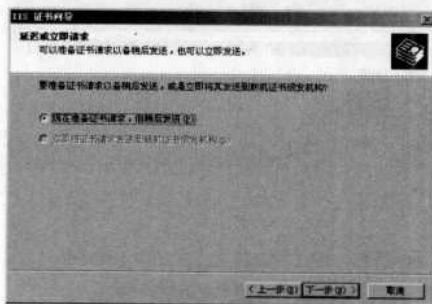
单击“服务器证书”按钮

STEP11在弹出的“欢迎使用 Web 服务器向导”中单击“下一步”按钮进入“服务器证书”对话框中选择“新建证书”后继续。



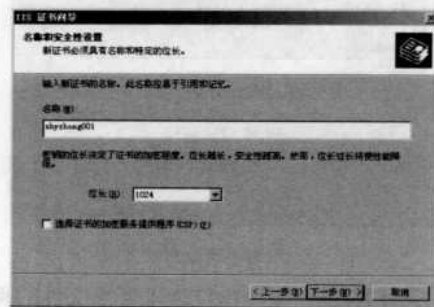
选择“新建证书”

STEP12出现“延迟或立即请求”对话框时，选择“现在准备证书请求，但稍后发送”项。



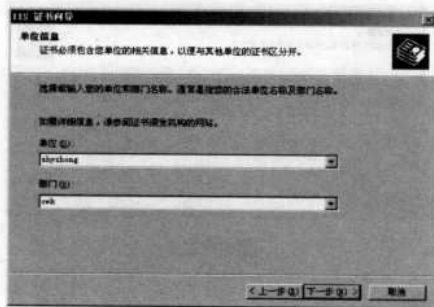
选择第一项

STEP13在下一步的“名称和安全性设置”对话框中，选择默认状态后继续。



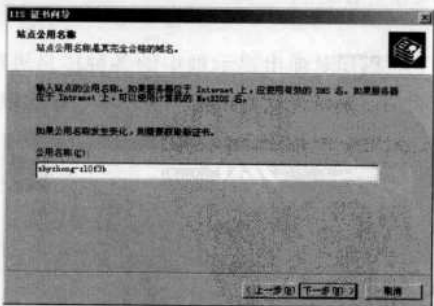
选择默认状态

STEP14在下一步的“单位信息”中，根据实际情况设置符合需求的证书的单位、部门名称。



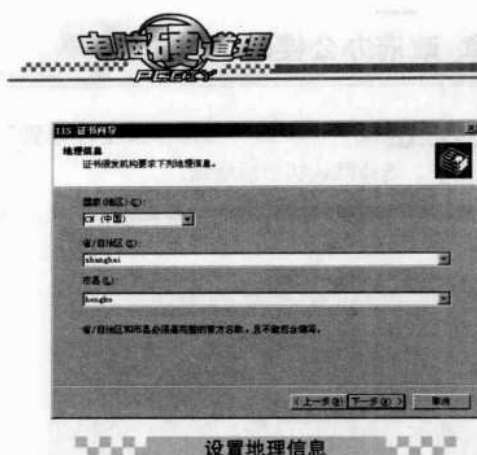
设置单位信息

STEP15在“站点公用名称”对话框中选择默认状态继续。

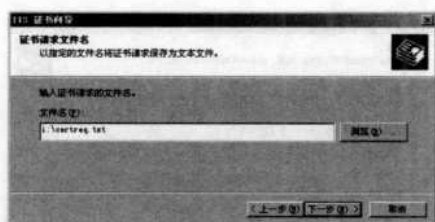


设置站点公用名称

STEP16下一步中需要设置站点的地理信息。



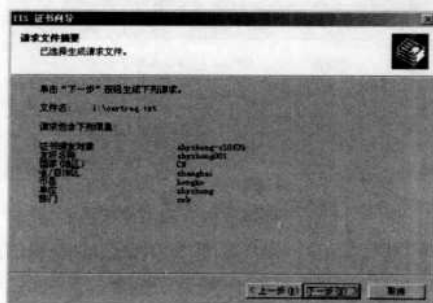
STEP17 现在需要指定请求证书文件的保存位置，为了充分发挥出 Windows Server 2003 的安全特性，建议将文件的保存路径设置在使用 NTFS 文件系统的分区中。这样就完成了请求证书文件的创建。



注意

牢记此文件的位置与文件名，因为在后面将要用到此文件中的信息。

STEP18 对弹出提示框中的各种信息进行逐一核对后，确认无误并单击“下一步”按钮继续。



166

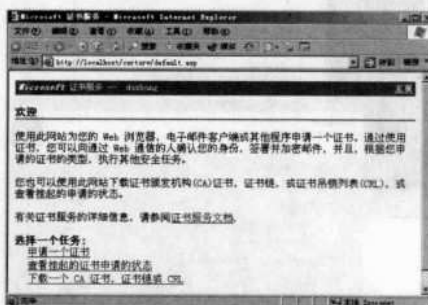
STEP19 在弹出的“完成 Web 服务器证书向导”中，单击“完成”按钮结束操作。



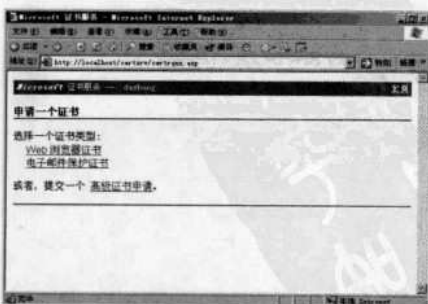
完成上述设置后，还要把创建的请求证书文件提交给证书服务器。操作如下：

首先在服务器端的 IE 浏览器地址栏中输入：
<http://localhost/CertSrv/default.asp>

STEP20 在弹出的“Microsoft 证书服务”欢迎窗口中单击“申请一个证书”链接。



STEP21 接下来在证书申请类型界面中，单击“高级证书申请”链接。

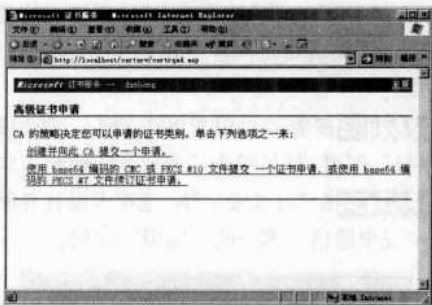


单击“高级证书申请”链接

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第八章 政府办公楼网络组建

STEP22在高级证书申请界面中，单击“使用 BASE64 编码的 CMC 或 PKCS#10...”链接。



单击第二项

STEP23打开上面生成的“certreq.txt”文件，使用“Ctrl+A”组合键将所有内容复制。



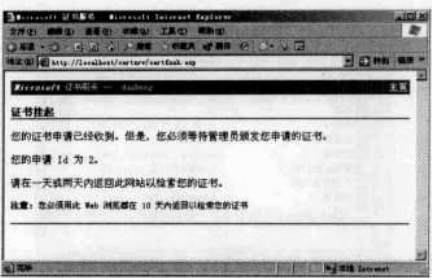
复制内容

STEP24接着将内容复制到“保存的申请”输入框后，单击“提交”按钮。



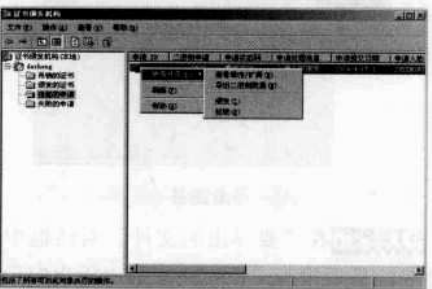
提交表单

STEP25从切换到的页面中可以看到上述的证书申请，服务器已经收到，此时需要等待管理员颁发申请的证书。



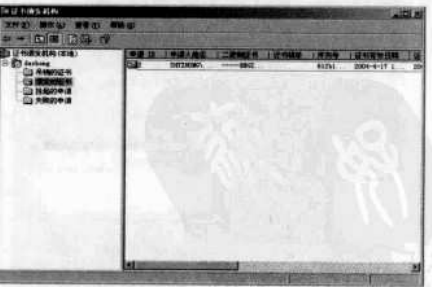
等待颁发

STEP26现在再来看看如何颁发服务器证书。依次单击“开始”→“设置”→“控制面板”→“管理工具”→“证书颁发机构”菜单项。在弹出的“”窗口中展开树状目录，单击“挂起的申请”项，从右侧部分可以看到刚才申请的证书。此时，使用右键选中并单击该项，在弹出的快捷菜单中选择“所有任务”→“颁发”。



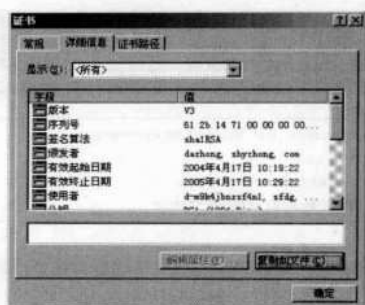
查看证书

STEP27颁发成功并单击树状目录中的“颁发的证书”项后，双击刚才颁发的证书。



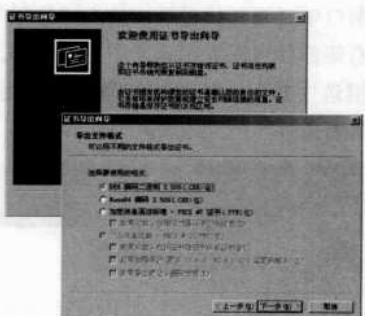
双击证书

STEP28在弹出的“证书”对话框的“详细信息”选项卡设置界面中，单击“复制到文件”按钮。



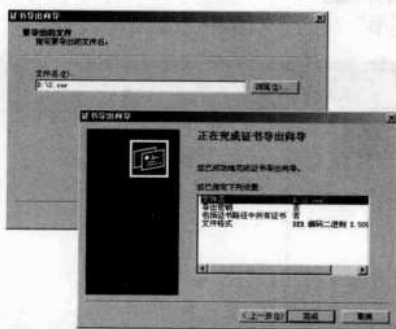
复制到文件

STEP29在稍后弹出的“证书导出向导”、“导出文件格式”页面中连续单击“下一步”按钮。



导出证书

STEP30在“要导出的文件”对话框中指定文件名，最后检查“正在完成证书导出向导”页面中检查信息无错后，单击“完成”按钮结束证书颁发操作。



完成颁发

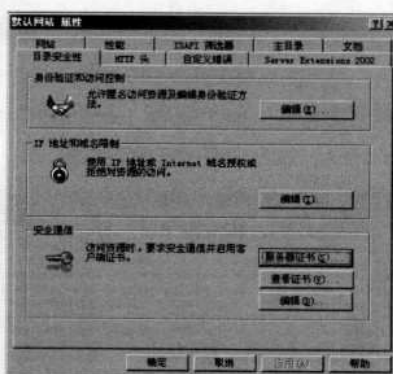
STEP31现在就可以进行安装服务器证书的操作了。首先进入使用 SSL 保护的网站属性页面，单击切换到“目录安全性”选项卡设置界面，单击“服务器证书”按钮，在弹出的“IIS 证书向导”

中进入“挂起的证书请求”对话框。

STEP32选择“处理挂起的请求并安装证书”选项后，单击“下一步”按钮进入“处理挂起的请求”对话框，这里请指定刚才导出的服务器证书文件的位置。

STEP33接着需要设置 SSL 端口，使用默认的“443”即可，最后单击“完成”按钮结束向导。

STEP34在“目录安全性”选项卡设置界面中，单击“安全通信”部分的“编辑”按钮。

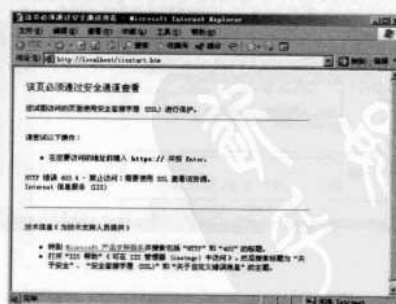


单击编辑

STEP35在弹出的勾选“要求安全通道 (SSL)”选项后，单击“确定”按钮即可启用 SSL。

8.4.3 访问SSL网站

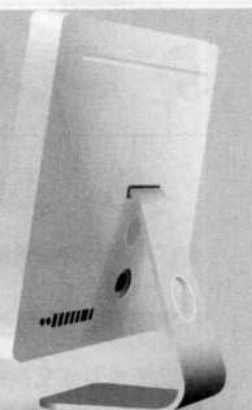
完成了对 SSL 网站的配置后，将无法使用“http://”格式进行 SSL 网站的访问。否则会出现如图所示的错误提示。



错误页面

根据提示，显然需要在 IE 浏览器中输入“https://”这样的格式（如 https://192.168.1.19/index.asp）才能访问网站。

第九章 网吧局域网组建实战



随着信息社会的发展，网吧这个概念早已风靡了全国的大街小巷，但同时，随着网吧的增多，行业之间的竞争也愈演愈烈，为了在激烈的竞争中立足，保证良好的网络运行高效性和稳定性，网络系统的性能在网吧的建设中就显得越来越重要。怎样才能保证网络系统 24 小时稳定工作，为用户提供一个舒适的、稳定的网络环境已成为网吧日益关注的重点。

9.1 网吧概述

Internet 飞速发展改变了人们生活方式。人们被无穷无尽的信息资源、方便快捷交流方式深深吸引，但是许多人不能方便地使用上网所需的电脑与其他设备。例如：住校学生、低收入的打工者，从而网吧就应运而生了。



网吧

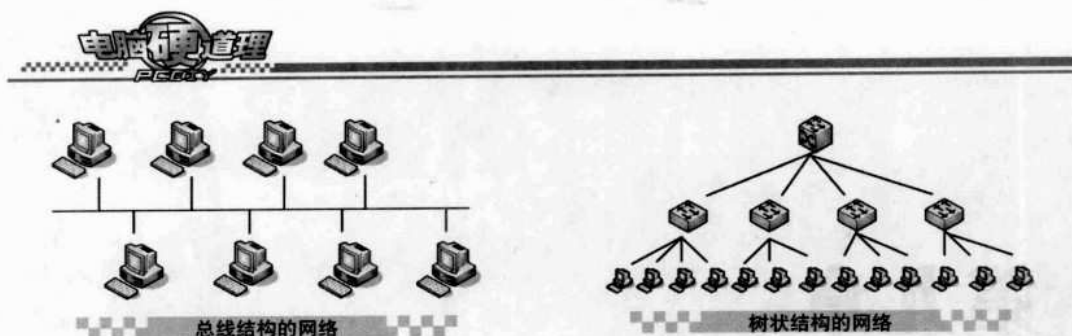
9.2 组建网吧的基本结构

组建局域网并不难，关键在于资金的问题，花多少钱，办多少事。普通的小型网吧没必要花

很多钱去组建一个硬件设施非常好的局域网，而且网络过于复杂的话，一方面是资源的浪费，另一方面是维护也比较麻烦。一般的经济网吧组网方式有两种，分别为总线型网络和星型网络。

9.2.1 总线型网络

具有一通到底的特性。总线结构的主要特性就是“用一条共有的网线来连接所有的发计算机”，这条很长的线是有“很多较短”的网线来连接的。它具有成本低和布线简单的优点。网络各节点通过简单的搭线器（T 头）即可接入网络。只要买足了网卡、网线、接头，就不需要其他格外的网络设备了。总线型网络适用于对网速要求不高单间房里有大量的节点相邻摆设的网吧。但总线型网络只能实现半双工功能，一次仅能一个端用户发送数据，其它端用户必须等待到获得发送权。媒体访问获取机制较复杂。而且不利于以后的扩展，是一种即将被淘汰的网络构架。当然，在一些落后和偏远地区，当受到资金限制的时候，这也是最佳的选择。



9.2.2 星型网络

它是以集线器或交换机为中心向外放射状，是通过集线器或交换机在各计算机之间传递信息的。其结构如图所示。该网络结构优点是局部线路故障只会影响到局部区域，不会导致整个网络的瘫痪，除非是集线器或交换机损坏。并且追查故障非常方便，通常从集线器或交换机的指示灯便能得知故障点。还有在增加或减少计算机时，不会造成网络中断，但必须增加一比购买集线器或交换机的成本。

星型网络的连接很简单，只要把制作好的双绞线一端插在主机网卡的 RJ-45 插口，另一端插到集线器或交换机上即可。按照此法把其它计算机连上集线器或交换机，即一个小型局域网的硬件连接到此完成。如果新增集线器或交换机，为了保证新增的集线器与原有的局域网结合，我们必须用“跳线”将两台集线器或交换机相连。



9.2.3 树状结构的网络

树状结构的网络的实质是星型结构网络的拓展，适合于较大规模的网吧环境，通过从接入层交换机到汇聚层交换机的树状链接，可以将网络的规模扩大若干倍。通常树状结构的网络需要依赖于少数性能较强的交换机，他们处于树状结构的根位置。

9.3 Internet的接入方式

Modem 拨号连接虽然价钱相对便宜但速度慢，频带宽度不足以应付网吧里的几十台电脑。对目前的网吧来讲已经是不具备实用价值的接入方式。在这里不予讨论，目前国内网吧接入解决方案最常见的技术有两种：

9.3.1 ADSL

ADSL(Asymmetrical Digital Subscriber Loop 非对称数字用户线环路)是 XDSL 家庭成员中的一员，被欧美等发达国家誉为“现代信息高速公路上的快车”。它是利用原有的电话线路来上网，但用户和电话控制的调制解调器必须更新成 ADSL 专用。

ADSL 最大的特点，就是理论上每秒能下载 8Mbit 的数据，是普通 56K 调制解调器的 150 倍，上行边达 640Kbps，频带宽度是普通电话用户频带的 256 倍以上，而且没有 ISDN 那么复杂的安装手续。

对于网吧用户来说，各地中国电信的收费是差不多的，通常无需交纳安装费，每月 100 元左右租金就可以获得 2mbps 的带宽。

此外，ADSL 是一种类似专线的连接，几乎永远在线，而它专用的连接又和 Cable Modem 不同。但是目前 ADSL 最大的争议就是其连接的速率会受到距离的影响。

一般来说，ADSL 可在 3000~5400 米之间传送，超过后就会发生传送出错的情况，速度也会随距离增远而降低。因此，网吧选址时还要考虑跟当地电信接入机房之间的距离。具体可以咨询当地的互联网接入商。

第九章 网吧局域网组建实战



ADSL Modem

现在网吧中使用 ADSL 作为上网线路的越来越多，一是因为 ADSL 比较便宜，另外是因为 ADSL 安装方便。但是 ADSL 的带宽有限，而网吧能否提供给用户高速稳定的上网线路，是能够留住顾客的关键。按照经验，如果是一条 512K 的 ADSL 线路，有 10 人同时频繁上网，就会明显感到不如单机电话拨号上网 (56K) 快；如果为 2M 线路，也只能勉强提供 30~40 人同时上网一般的质量；8M 也只能保证 100 人同时上网几乎接近于电话线拨号的效果。

很多网吧的经营者都在寻找经济有效的扩容办法。增加 ADSL 线路是一个常用的办法。但增加之后，怎样才能不破坏整个网吧局域网的互通性能呢？怎样才能方便地进行管理？怎样才能分配好在两条 ADSL 线路上的机器数量呢？一般说选用支持两条 ADSL 线路的宽带路由器是一种直觉的思路，但是要实现负载均衡的宽带路由器往往价格昂贵，而且在网吧机器多的情况下宽带路由器的 CPU 处理能力可能成为瓶颈。

笔者推荐一种简单易行、经济实用的方案。使用两台高性能的宽带路由器和有 VLAN 功能的交换机，以较低的价格获得较好的应用效果。

9.3.2 光纤线路

光纤接入是指局端与用户之间完全以光纤作为传输媒体，光纤接入可以分为有源光接入和无源光接入。光纤用户网的主要技术是光波传输技术。光纤接入是一种理想的宽带接入方式，可以很好的解决宽带上网的问题，速度快、障碍率低、抗干扰性强。并且光纤链路的上行和下行速度是

一样的，比 ADSL 有较大优势。当然，光纤链路的价格也比 ADSL 线路昂贵很多，通常是较大规模的网吧采用。

近年来，以互联网为代表的新技术革命正引领着传统的电信概念和结构体系向一个全新的方向发展，随着各国接入网市场的逐渐开放以及电信管制政策的日渐放松，新业务需求在越演越烈的地盘争霸战中层出不穷，在巨大的市场潜力驱动下，产生了各种各样的接入网技术，有线接入和无线接入等技术的不断成熟加快了各自的商用步伐。网吧乘此风迅速崛起而呈现出遍地开花之势，随着网吧的增多，行业之间的竞争也越来越激烈，要在激烈的竞争中立于不败之地，设计和组建一个稳定、高速、便于管理控制的低投资高收益的网吧网络就显得极其重要，而选择一种合适网络接入方式则是实现此举的关键，路由器、交换机等网络设备的选购也是相当重要的。

网吧网络应用类型非常的多样化，对网络带宽、传输质量和网络性能有很高的要求，网络应用要集先进性、多业务性、可扩展性和稳定性于一体，不仅满足顾客在宽带网络上同时传输语音、视频和数据的需要，而且还支持多种新业务数据处理能力，上网高速通畅，大数据流量下不掉线、不停顿等。在众多的 Internet 接入方式中，光纤接入以其独特的带宽优势脱颖而出，作为信息化发展时代的快速通道，成为众多网吧经营者的理想选择。选择光纤接入的组网方案也是目前宽带应用中的最佳组网方案。

大致的组网方案如下：

(1) 光纤直接接到网吧，然后通过一光纤收发器将光信号转换成 10M/100M 电信号。接入采用光纤，速度快、稳定性好、障碍率低、抗干扰性强。

(2) 用一路由器作为局域网的网关，此路由器在功能与性能上必须满足网吧网络的需求，由于它是专门用于路由转发、地址映射的硬件设备，在工作效率上比电脑主机强百倍，且具有非常优异的稳定性。此路由器需具备双以太网口：一个用于与光纤收发器连接，另一个用于与交换机连接，连接介质均为网线。路由器作网关，路由转发能力强，



稳定性好、具有很高的安全性，可以确保局域网内部机器安全上网无后顾之忧，而且可以保持长期在线。

(3) 用一交换机用于局域网内部互连。与集线器的共享总线式带宽相比，交换机使用独享式带宽，在功能和性能上远远超过集线器。交换机可以大大提高网络利用率，减少局域网内部冲突，提高上网速度。尤其是在较多机器同时运行的情况下，交换机发挥的作用将更大。

9.4 网吧基础硬件

9.4.1 工作站计算机

工作站实际上就是普通的电脑，07 年的网吧工作站计算机基本已经过渡到酷睿 2 双核以上档次的电脑。由于网吧的需求特殊，对成本控制也要求较高，因此 90% 以上的网吧都选择了 DIY 攒机，而非品牌厂商的产品。具体操作时一般根据资金、应用等具体情况使用当时流行配置的电脑作为工作站。网络工作站可以不配置软驱和光驱，而且硬盘可以选择容量较小的，这样不仅可以充分利用服务器的资源，节省资金，还可防止病毒感染，保证网络安全。

以下是以市场参考为标准的主流网吧用计算机的配置清单：

1.经济型配置

这套配置虽然硬件档次较低，但是依然可以满足绝大部分游戏和应用需要，并且使用了大量集成设备，因此耗电量较低，对于网吧来说大量配置这样的计算机可以有效的降低每月的电费成本。当然对于竞争激烈的繁华地区，拥有众多游戏发烧友的高校周边，这样的配置可能并不能收到客户欢迎。

配件名称	型号	价格(元)
CPU	AMD Athlon 64 X2 4000+ (盒)	425
散热器	盒装自带	—
主板	华擎 ALiveNF7G-HD720p R3.0	365
内存	现代 1GB DDR2 667	110
硬盘	日立 160GB 8M SATA	365

显卡	主板集成	—
声卡	主板集成	—
网卡	主板集成	—
显示器	另配	—
耳机	随机赠送	—
光驱	—	—
机箱	多彩 DLC-A016魔兽	180
电源	机箱自带	—
鼠标、键盘	力胜 KB-60黑豹2键盘光学套装	45
合计		1490

2.豪华型配置

这套配置采用了相对主流的硬件产品，基本可以满足未来一段时间出现的游戏和业务需要，17 寸液晶显示器也是目前网吧配置的主流。可以博得游戏玩家和网迷的亲睐，在竞争激烈的地域赢得更多用户。

配件名称	型号	价格(元)
CPU	AMD Athlon 64 X2 4000 (盒)	800
散热器	盒装自带	—
主板	升技NV8	650
内存	现代 1GB DDR2 667×2	220
硬盘	日立 160GB 8M SATA	365
显卡	翔升擂神x700	700
声卡	主板集成	—
网卡	主板集成	—
显示器	AOC 17 LCD宽屏	1450
耳机	硕美科	25
光驱	—	—
机箱	多彩 MF431 38度机箱	180
电源	长城350W	100
鼠标、键盘	罗技光电套装	145
合计		4635

以上配置和报价仅供参考，实际价格和产品信息可能有较大变化。总之选择网吧计算机时，各种配件应该选择品质过硬的品牌产品，尤其是键盘、鼠标等与用户直接交互的产品，电源、主板等易损坏品。否则在经营过程中较低的客户感受和频繁维护会给网吧业主带来更大的损失。

而对于一些定位与高端用户群的网吧，如白领聚居区、写字楼区、高档酒店、咖啡厅、机场等场所的网吧，则应当以各种品牌计算机为选择对象。国内品牌如联想、方正、国外品牌如 DELL 等，都可以提供价格较低而拥有较高档次的网吧专用计算机产品，同时品牌厂商的服务还可以大大降低网吧业主对设备维护的投入。

第九章 网吧局域网组建实战



方正网吧专用机

9.4.2 网吧服务器

大多数时候服务器是网络中提供各种服务和功能的高性能计算机。作为网吧服务器可以采用一般配置较高的普通电脑，也可以采购更加高端的专用工作组级别服务器，注意内存和硬盘的容量应适当大一点，而在显卡、显示器等方面则不必过多花费。如果服务器要负载在线电影等大量读取数据的业务，还应当为服务器选购磁盘阵列设备，甚至安装专门的磁盘阵列机。同时服务器的数量也应该按照实际服务种类和业务规模而定。

以下为 Dell PowerEdgeTM 840 塔式工作组服务器配置信息：

CPU：双核 3050 处理器，2MB 缓存，2.13GHz，至强 1066MHz 前端总线

内存：1G DDR-2 667MHz ECC 1R 内存

硬盘：SATA II 160G 7.2K RPM

光驱：CD

网卡：内置千兆 以太网

显卡：集成 ATI RN50 VGA 控制器

声卡：无

I/O：普通

2 个 64 位 /133MHz PCI-X 插槽

1 个 x1 PCI Express 插槽

1 个 x8 PCI Express 插槽

1 个 32 位 /33MHz 5v 老式插槽

所有插槽均悉全高全长。这样一台服务器的售价大约在人民币 6000 元左右，可以满足大部分网吧服务的需要，如：计费、游戏服务、在线电影、监控等。



Dell PowerEdge 840服务器

9.4.3 网络传输介质

常见的网线分细同轴电缆、粗同轴电缆和双绞线、光缆等。以前同轴电缆采用较多，主要是因为同轴电缆组成的总线形结构网络成本较低，但单条电缆的损坏可能导致整个网络瘫痪，维护也难，这已经是一种将近淘汰的网络形式。

以下重点介绍双绞线。根据最大传输速度的不同，双绞线分为不同的类别：3 类、5 类及超 5 类。3 类双绞线的速率为 10Mb/S，5 类双绞线的速率可达 100Mb/S，超 5 类更可达 155Mb/s 以上，可以适合未来多媒体数据传输的需求。双绞线还分为屏蔽双绞线（STP）和非屏蔽双绞线（UTP），STP 双绞线内部包了一层皱纹状的屏蔽金属物质，并且多了一条接地用的金属铜丝线，因此它的抗干扰性比 UTP 双绞线强，但价格也要贵很多。对于 UTP 双绞线，阻抗值在 1MHz 时通常为 100 欧姆，中心芯线 24AWG（直径为 0.5mm），每条双绞线最大传输距离为 100 米。由于网线布线大多涉及到建筑结构 with 内部装修，因此在布线完成后，如果想重新布线是非常困难的，所以即使网卡等设备还是 10Base-T 的，但是在规划网络时，应该考虑到未来的需求，所以应采用 5 类甚至 5 类的双绞线。

和双绞线配套使用的还有 RJ45 水晶头，用于制作双绞线与网卡 RJ45 接口间的接头，其质量好坏直接关系到整个网络的稳定性，不可忽视。推荐选用 AVAYA、AMP 等知名厂家的产品。



双绞线

9.4.4 集线器和交换机

现在网吧的数据交换中心无疑是 HUB（集线器）和交换机，那么集线器和交换机到底有什么不同呢？

HUB 是工作在 OSI 模型的在底层物理层上面，集线器可以看成是一种多端口的中继器，是共享带宽式的，其带宽由它的端口平均分配，如总带宽为 10Mb/s 的集线器，连接 4 台工作站同时上网时，每台工作站平均带宽仅为 $10/4=2.5\text{Mb/s}$ 。它只是能够简单的提供各个终端数据之间的传送和分发，而不是去识别数据包头的指向，也就是说，它接收到一个包后，是把这个包分别发送给它所所有的端口去识别，而不是象邮递员一样，准确的去投递。传输通过碰撞检测进行，同一网段计算机越多，传输碰撞也越多，传输速率会变慢。所以，尽管集线器价格低廉，但是因为其糟糕的工作性能，已经逐渐被人们所遗弃，目前网吧所使用的网络数据交换中心通常是各种型号的交换机。



集线器

交换机是工作在数据链路层的，它在局域网内可以智能的识别包头的指向，并且准确无误的发送到目的地。交换机又叫交换式集线器：可以

想象成一台多端口的桥接器，每一端口都有其专用的带宽，如 100Mb/s 的交换式集线器，每个端口都有 100Mb/s 的带宽。传输速率不受计算机增加影响，其独特的 NWAY 全双工功能增加了交换机的使用范围和传输速度。

现在交换机和集线器普遍采用了自适应（Auto-sense 或 Auto-Negotiation）技术。可以自动适应 100M 和 10M 速率。这类交换机和集线器按照多种规则适应工作速率：100M 全双工，100M 半双工，10M 全双工 10M 半双工。Auto-Negotiation 在 IEEE 802.3u 中已有规定。其好处是在不需用户参与设定的情况下，自动以最高速率连接。交换机和集线器都遵循 IEEE802.3 或 IEEE802.3u，其介质存取方式均为 CSMA/CD。交换机无论在各个方面表现的都要比 HUB 要优秀很多。所以一般都选取交换机作为主要的交换设备。



交换机

9.4.5 网吧路由器

要解释路由器的概念，首先要介绍什么是路由。所谓“路由”，是指把数据从一个地方传送到另一个地方的行为和动作，而路由器，正是执行这种行为动作的机器，它的英文名称为 Router。是使用一种或者更多度量因素的网络层设备，它决定网络通信能够通过的最佳路径。路由器依据网络层信息将数据包从一个网络前向转发到另一个网络。实际上在绝大部分的网吧应用中，并不会用到真正的路由器，因为网吧的计算机通常并没有在 Internet 上合法的 IP 地址。因此在网吧中使用的路由器实际上是一个带有 NAT 功能的网络出口设备，他能将网吧中大量的计算机数据转换成出口上的一个 IP 地址进行转发，并将外界的数据传入网吧内部，相当于网吧线路的出口。

网吧路由器往往可以直接连接 ADSL Modem

第九章 网吧局域网组建实战

甚至可以直接连接光纤线路，这是由网吧路由器的档次决定的。

在很多网友眼中，好像双 WAN 和多 WAN 路由器就是专门给网吧使用的，因为可以接入多根宽带线扩充带宽，又可以接入多个 ISP 运营商的网络实现访问南方站点同时提速，非常符合网吧上网的需求嘛。其实不然，不少双 WAN 多 WAN 路由器其实是通用型的，既可以在企业网络中使用，也可以在网吧环境下使用，但是通用型的产品大部分都存在针对性不强的问题，例如功能方面，可能就会缺少一些专门针对网吧工作环境而设计的功能，那么，专门针对网吧工作环境而设计的自然就是专业级的网吧路由器了，这类产品能不能用在企业网络，当然可以。记得一个台湾网络设备供应商的技术工程师说过：“中国的网吧可以说是世界上网络应用环境最复杂的场所，如果一款路由器能够在中国的网吧中良好的使用，那么把它拿到其他同规模的接入环境下肯定也能很好的使用”，既然如此，专业级的网吧路由器岂不是非常彪悍？是的，所以这类产品价格也相对要高一些，不过也算物有所值。

一般来说，有那么几个功能是专业级双 WAN 网吧路由器所具备的：

策略路由：既然是双 WAN，自然很多时候会接入电信和网通两条线，这样的话，如何让访问电信服务器的时候走电信的线出去，访问网通网站的时候走网通的线出去，就需要策略路由来实现，一般是通过一个预置的静态路由表来实现，设备供应商先把电信和网通的 IP 段划分好存在表里面，然后判断用户访问的网站 IP 是属于电信的还是网通的，如果是电信的，自然就走接电信线路的那个 WAN 口，反之，所以服务商的这个静态路由表就是关键，它包含的 IP 地址越准确，所支持的运营商越多，效果就越好。

端口镜像：出于安全管理的需要，对绝大部分地区的网吧公安局都要求有一个镜像监听端口，以配合专用软件对内网的访问进行监控，专业级网吧路由器会有一个 LAN 口可以用作镜像端口，通过这个端口可实现端口流量控制，数据安全分流，还有独特的数据监听，网内信息可通过

公安部门监督，加强网络管理。如果没有这个端口，网吧就需要再去购买一台用于做镜像端口的镜像交换机，所以专业级网吧路由器的端口镜像功能应该说是必备的。

IP-MAC 绑定：自从年初 ARP 局域网病毒大肆泛滥导致网吧大面积断网之后，很多路由器产品都开始内置这个功能，以实现内网的安全稳定，当然这个功能很多商用路由器之前都提供有，但是需要手动去绑定，一个网吧几百台电脑，每个去绑定确实是累坏网管，而最新上市的专业级网吧路由器不少都将这个绑定过程自动化了，大大减轻网管的工作负担。



网吧路由器

9.5 大型网吧网络组网方案

接下来，我们以部署在某大城市商业中心的一个大型网吧建设为例，为大家介绍网吧网络构建过程，该网吧的营业面积大约为 1500 平米左右。

9.5.1 需求分析

大型网吧网络系统建设的主要目标是建设成为主干千兆，百兆交换到桌面；同时在大型网吧的范围内建立一个以网络技术、计算机技术与现代信息技术为支撑的娱乐、管理平台，将现行以游戏网为主的活动发展到多功能娱乐这个平台上来，籍以大幅度提高网吧竞争和盈利能力，建设成一流的高档网吧，为吸引高端消费群打下强有力的基础。

按照这一目标，大型网吧网络系统的主要目标和任务是：

(1) 在大型网吧管辖范围内，采用标准网络协议，结合应用需求，建立大型网吧内联网，并通过中国电信宽带网与 Internet 相连；



(2) 大型网吧内联网上建立支持娱乐活动的服务器群（包括 WWW、FTP、DNS、流媒体服务器、各种游戏战网服务器等），具有信息共享、传递迅速、使用方便、高效率等特点的处理系统；

(3) 视市场环境允许，向中、小型网吧及网络固定客户提供服务器群资源有偿共享服务，在小范围内尝试为小私营企业主提供一体化网站解决方案（空间、域名、网站、数据库及更新等）；

(4) 系统应有高可靠性、安全性、可维护性和可扩充性，要具有良好的用户界面。

本方案的设计过程中，始终以大型网吧建网的实际需求为主要参考，在较充分地了解大型网吧应用需求的基础上，根据网络建设中的相关技术路线和建设方针，最终完该的方案设计。

9.5.2 网络设计原则

大型网吧网络系统建设是一项大型网络工程，各网吧需要根据自身的实际情况来制定网络设计原则。在大型网吧的网络建设过程中，其遵循以下网络设计原则：

1.实用性和经济性

由于网吧一次性资金投入大，设备折旧快，目前外部经营环境差。另一方面，网吧应用环境比较恶劣，顾客应用水平较参差不齐，因此，在网络的建设过程中，系统建设应始终贯彻面向应用，注重实效的方针，坚持实用、经济的原则。

2.先进性和成熟性

当前计算机网络技术发展很快，设备更新淘汰也很快。这就要求网络建设在系统设计时既要采用先进的概念、技术和方法，又要注意结构、设备、工具的相对成熟。只有采用当前符合国际标准的成熟先进的技术和设备，才能确保网络能够适应将来网络技术发展的需要，保证在未来几年内占主导地位。

3.可靠性和稳定性

在考虑技术先进性和开放性的同时，还应从系统结构、技术措施、设备性能、系统管理、厂商技术支持及维修能力等方面着手，确保系统运行的可

靠性和稳定性，达到最大的平均无故障时间。

4.安全性和保密性

系统设计中，既考虑信息资源的充分共享，更要注意信息的保护和隔离，因此系统应分别针对不同的应用和不同的网络通信环境，采取不同的措施，包括系统安全机制、数据存取的限制控制等。

5.可扩展性和易维护性

为了适应系统变化的要求，必须充分考虑以最简便的方法、最低的投资，实现系统的扩展和维护。把当前先进性、未来可扩展性和经济可行性结合起来，保护以往投资，实现较高的总体性能价格比。

9.5.3 设备选型和预算

1.计算机

为满足大城市年轻人群的激进需求，必须拥有较高配置的计算机，以完成各种时尚游戏、网络娱乐业务。液晶显示器也是目前主流网吧所必备，以提高网吧整体档次和形象，吸引更多客户。同时又要有效的控制成本，不能一味追求高新配置。因此在该次设备选型中，我们选择了如下配置的计算机作为该网吧建设用机：

配件名称	型号	价格(元)
CPU	AMD Athlon 64 X2 4000+（盒）	800
散热器	盒装自带	—
主板	升技NV8	650
内存	现代 1GB DDR2 667×2	220
硬盘	日立 160GB 8M SATA	365
显卡	翔升擂神x700	700
声卡	主板集成	—
网卡	主板集成	—
显示器	AOC 17 LCD宽屏	1450
耳机	硕美科	25
光驱	—	—
机箱	多彩 MF431 38度机箱	180
电源	长城350W	100
鼠标、键盘	罗技光电套装	145
合计		4635

该型计算机采购数量为一次性 300 台，要求设备供应商提供 1 年的上门质量保证，并进行严格的测试，按时送货。

第九章 网吧局域网组建实战

2. 网吧服务器

按照网吧建设规划，网吧将为客户提供各种网络服务，因此按照服务需求，计划采购服务器如下：

用途	型号	配置	价格
管理和计费	DellPower Edge 840	2.13/1G/160G SATA	6000元
Web服务、流媒体	DellPower Edge 1403	2*4核5310/2G/SCSI+RAID640G	10500元
游戏服务器	DellPower Edge 840	2.13/1G/160G SATA	6000元

服务器选用国际品牌 Dell，拥有一流的品质，良好的服务和相对低廉的价格，整体采购，享受3年上门服务，使得网吧的核心业务得到充足保障。

3. 网络线缆

由于网络线缆需要在装修时预埋，无法再后期维修和更换，因此选择质量上乘的品牌网线为佳。

9.6 大型网吧网络系统方案实施

方案实施共分为五部分：

1. 综合布线系统；
2. 操作系统安装；
3. Internet 接入；
4. 收费系统；
5. 服务器系统。

9.6.1 综合布线系统布线原则

1. 抗干扰

综合布线在布线设计时，应当综合考虑电话线、电力线和双绞线的铺设。电话线和电力线不能离双绞线太近，以避免对双绞线产生干扰，但也不宜离得太远，相对位置保持 20cm 左右即可。

2. 注重美观

网吧布线更注重美观，因此，布线施工应当与装修时同时进行，尽量将电缆管槽埋藏于地板或装饰板之下，信息插座也要选用内嵌式，将底盒埋藏于墙壁内。

3. 简约设计

由于信息点的数量较多，为方便管理，应该

集中管理。所以网吧布线可以使用配线架。双绞线的一端连接至信息插座，另一端则连接至集线设备，从而减少管理难度。

4. 适当冗余

综合布线的使用寿命为 15 年，但是网吧计算机数量较多，且随着网吧业务的不断扩大，可能需要更多的信息点。所以，适当的冗余是非常有必要的。

双绞线布线方法：

首先是“放线”，确定网络集线设备和每台计算机之间的距离，分别截取相应长度的网线，然后将网线穿管（PVC 管）沿着墙壁线槽走线。要注意的是双绞线（网线）的长度不得超过 100 米，否则就得加装中继器来放大信号。

接着是“做网络接头”，也就是制作 RJ45 双绞线接头。在讲述如何正确接线之前，要先说明 8 根双绞线的编号规则。编号次序是这么定义的：把 RJ45 有卡子的一面向下，8 根线镀金脚的一端向上，从左起依次为 12345678。

EIA/TIA-568 标准规定了两种连接标准（并没有实质上的差别），即 EIA/TIA-568A 和 EIA/TIA-568B。

T568A 规定的连接方法是：

- 1—— 白 - 绿（就是白色的外层上有些绿色，表示和绿色的是一对线）
- 2—— 绿色
- 3—— 白 - 橙（就是白色的外层上有些橙色，表示和橙色的是一对线）
- 4—— 蓝色
- 5—— 白 - 蓝（就是白色的外层上有些蓝色，表示和蓝色的是一对线）
- 6—— 橙色
- 7—— 白 - 棕（就是白色的外层上有些棕色，表示和棕色的是一对线）
- 8—— 棕色

T568B 规定的连接方法是：

- 1—— 白 - 橙（就是白色的外层上有些橙色，表示和橙色的是一对线）
- 2—— 橙色



3——白-绿（就是白色的外层上有些绿色，表示和绿色的是一对线）

4——蓝色

5——白-蓝（就是白色的外层上有些蓝色，表示和蓝色的是一对线）

6——绿色

7——白-棕（就是白色的外层上有些棕色，表示和棕色的是一对线）

8——棕色

这两种标准的连接方法如图所示。



T568A

T568B

双绞线的制作标准

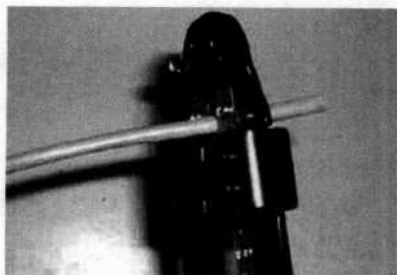
具体制作步骤为：

STEP 1 准备好 5 类线、RJ45 插头和一把专用的压线钳。



制线工具

STEP 2 用压线钳的剥线刀口将 5 类线的外保护套管划开（小心不要将里面的双绞线的绝缘层划破），刀口距 5 类线的端头至少 2 厘米。



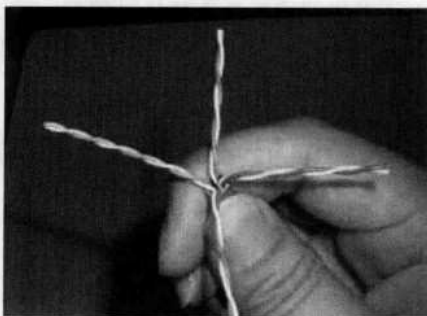
剥去头部保护套管

STEP 3 将划开的外保护套管剥去（旋转、向外抽）。



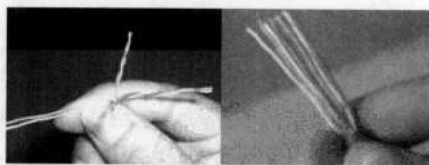
剥去划开的保护套管

STEP 4 露出 5 类线电缆中的 4 对双绞线。



露出 5 类线电缆

STEP 5 小心的剥开每一对线，因为我们是遵循 EIA / TIA 568B 的标准（白橙-橙-白绿-蓝-白蓝-绿-白棕-棕）排列好。



EIA / TIA 568B 标准

STEP 6 将裸露出的双绞线用剪刀或斜口钳剪下只剩约 1.4 厘米的长度，之所以留下这个长度是为了符合 EIA / TIA 的标准，您可以参考有关用 RJ45 接头和双绞线制作标准的介绍。最后再将双绞线的每一根线依序放入 RJ45 接头的引脚内，第一只引脚内应该放白橙色的线，其余类推。

第九章 网吧局域网组建实战



9.6.2 操作系统安装

操作系统的安装主要分为网吧客户机系统的安装和网吧服务器系统的安装两部分。在这里网吧客户机系统我们安装目录流行的 Windows XP Professional SP2；网吧服务器系统我们安装 Windows 2003 Server SP2。

网吧客户机系统的安装

Windows XP 具有运行可靠、稳定而且速度快的特点，它不但运用更加成熟的技术，而且外观设计趋紧清新明快，使用户有良好的视觉享受。XP 系统增强了多媒体性能，使媒体播放器与系统完全融为一体，用户无需安装其他的多媒体播放软件，就可以播放和管理各种格式的音频和视频文件。Windows XP 系统中包含的众多的技术和功能，使用户能轻松地在其环境下完成各种管理和操作。

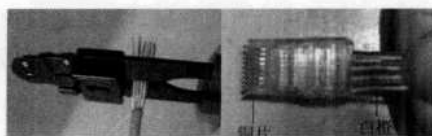
1.准备工作:

- (1) 准备好 Windows XP Professional SP2 简体中文版安装光盘，并检查光驱是否支持自启动。
- (2) 可能的情况下，在运行安装程序前用磁盘扫描程序扫描所有硬盘检查硬盘错误并进行修复，否则安装程序运行时如检查到有硬盘错误即会很麻烦。
- (3) 用纸张记录安装文件的产品密钥（安装序列号）。
- (4) 记下主板、网卡、显卡等主要硬件的型号及生产厂家，预先准备驱动程序备用。
- (5) 如果你想在安装过程中格式化 C 盘或 D 盘（建议安装过程中格式化 C 盘），请备份 C 盘或 D 盘有用的数据。

2.用光盘启动系统:

（如果你已经知道方法请转到下一步），重新启动系统并把光驱设为第一启动盘，保存设置并重启。将 XP 安装光盘放入光驱，重新启动电脑。刚启动时快速按下回车键，否则不能启动 XP 系统光盘安装。

接着按照常规步骤安装 Windows XP Professional 即可。安装完成后自动重新启动，出现启动



将双绞线放入RJ45水晶头

STEP 7 确定双绞线的每根线是否按正确顺序放置，并查看每根线是否进入到水晶头的底部位置。



检查水晶头

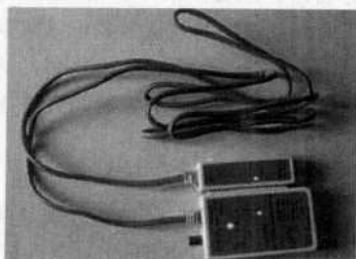
STEP 8 用 RJ45 压线钳压接 RJ45 接头，把水晶头里的八块小铜片压下去后，使每一块铜片的尖角都触到一根铜线。



压接过程

STEP 9 重复步骤 1 到步骤 6，再制作另一端的 RJ45 接头。因为工作站与集线器之间是直接对接，所以另一端 RJ45 接头引脚接法完全一样。

STEP 10 最后用测线仪测试网线和水晶头是否连接正常，如果两组 1、2、3、4、5、6、7、8 指示灯对应的灯同时亮，表示双绞线制作成功。



测试连接性



画面，接下来是欢迎使用画面。



欢迎信息

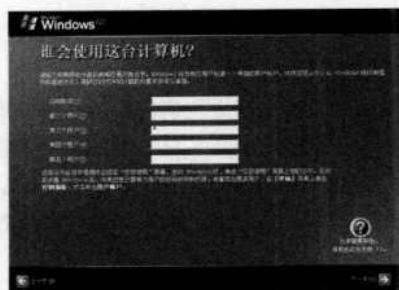
点击右下角的“下一步”按钮，出现设置上网连接画面。



选择上网连接方式

这里建立的宽带拨号连接，不会在桌面上建立拨号连接快捷方式，且默认的拨号连接名称为“我的ISP”（自定义除外）；进入桌面后通过连接向导建立的宽带拨号连接，在桌面上会建立拨号连接快捷方式，且默认的拨号连接名称为“宽带连接”（自定义除外）。如果你不想在这里建立宽带拨号连接，请点击“跳过”按钮。

已经建立了拨号连接，就可以激活XP啦，不过即使不激活也有30天的试用期，选择“否，请等候几天提醒我”，点击“下一步”按钮。



配置用户名

输入一个你平时用来登录计算机的用户名，点“下一步”后再点击完成，就结束安装。系统将注销并重新以新用户身份登录。

网吧服务器系统的安装

Windows Server 2003 操作系统（内部版本号是 Windows NT 5.2）是在 Windows 2000 Server 操作系统基础上发展而来的。业内也把 Windows Server 2003 操作系统称做是 Windows 2000 Server 的 .NET 版。2003 年 4 月份微软第一次发布 Windows Server 2003 的时候，曾把这款操作系统软件命名为 .NET Server 2003。与 Windows 2000 类似，Windows Server 2003 操作系统软件也分成多个版本针对不同用户发布。

例如：企业版和数据中心版的 Windows Server 2003 就是面向集群应用和负载均衡类关键用户的，它们还具有 64 位版本，只针对 Intel 的 IA-64 架构。Web 版的 Windows Server 2003 则专门针对网站类用户使用。Web 版的 Windows Server 2003 操作系统软件最多只能同时支持 2 颗处理器和 2GB 内存，如果同时需要支持 32 颗处理器和 128GB 内存，则必须购买 64 位的数据中心版 Windows Server 2003 软件。64 位企业版 Windows Server 2003 最多只能支持 8 颗处理器和 64GB 内存（32 位版本则支持的最大内存减半）。

标准版的 Windows Server 2003 软件最多可以支持 2 路处理器和 4GB 大小的内存。由此可以看出，购买微软的软件，尤其需要看清楚版本，版本不同，提供的功能也会有很大的差别。

Windows Server 2003 默认安装后，将不启用任何服务模块，用户需要对 Windows Server 2003 进行服务器角色配置，来开启相应的服务模块。不起用任何服务模块的默认安装可以减少系统受攻击的风险。Windows Server 2003 中的 AD 也做了增强和改进，对 NT、XP 系统的升级迁移提供了良好的帮助。

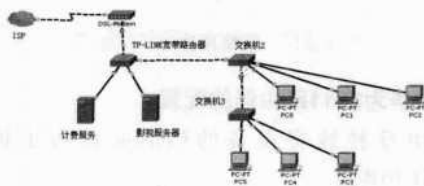
在网吧网络系统方案中我们可以选择 Windows Server 2003 企业版就可以满足网吧的需求。其安装过程跟上面的 windows XP 安装类似，在这里我们就不在赘述。

第九章 网吧局域网组建实战

9.6.3 Internet接入设备配置

在前面的课程中我们谈到目前网吧在我国主要有 ADSL 和光纤专线接入两种方式。在本节中，我们主要讲解这两种方式接入 Internet 时，各设备的一些配置。

(一) 通过ADSL共享上网配置



ADSL共享上网拓扑图

1.TP-LINK宽带路由器的配置

进入路由器 web 管理页面，路由器出厂是都有一个默认的 IP，具体的查看说明书即可，这里假设该 IP 是 192.168.10.1，连接之前需要将 PC 机的 IP 设成跟路由器的 IP 在同一个网络内，例如 192.168.10.2，然后在 IE 地址栏输入 http://192.168.10.1，会弹出如图所示的登录窗口，输入用户名和密码（说明书上都有），确认后即可进入。



登录宽带路由器



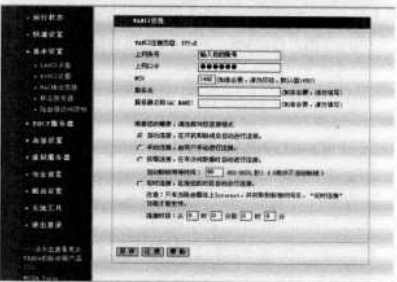
进入宽带路由器配置界面

选择“网络参数”→“LAN 口设置”，设置一个 IP 地址，也可以使用默认的，设置好之后保存即可。



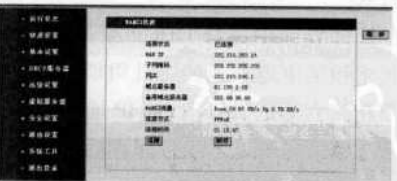
设置LAN口IP地址

选择 WAN 口设置，连接类型选 PPPOE，上网账号和口令是网络服务商提供的，然后选择一种连接模式，包月一般选择自动连接即可，对于计时收费的用户，不要选择自动连接，可以选择按需连接或者手动连接。输入完后点击连接即可。



配置WAN连接

这时点击运行状态如果看到图中所示信息，就表示连接成功。



连接成功

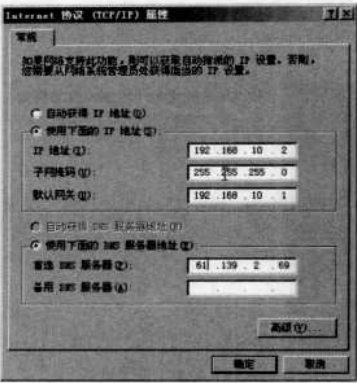
2.服务器以及客户机上网的配置

服务器以及客户机的设置如下：IP 设置为 192.168.10.x，各机器不要重复即可，子网掩码 255.255.255.0，网关设成路由器的 LAN 口 IP 地址，即 192.168.10.1，DNS 可以从路由器的连接状态

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

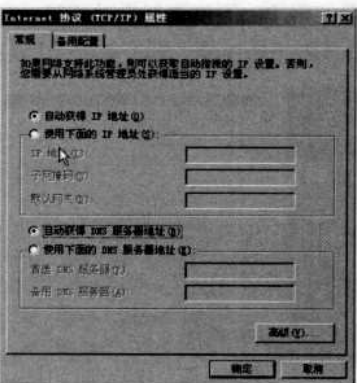


中看到。



服务器以及客户机上网的配置

另外，客户机也可以选择自动分配 IP 的方式，不需要手工设置 IP。



自动获取 IP 地址

前提是路由器启用了 DHCP，启用 DHCP 的方法如下：

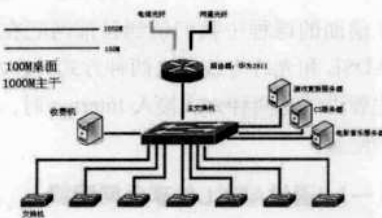
在管理界面中选择 DHCP 服务，选择启用，输入起始和结束地址池和地址租期，地址池的地址必须和路由器的 LAN 口的 IP 地址在同一个网络内，选填内容可以不填，保存后重启一下路由器即可。这样，用户就不需要手动设置 IP，开机后会自动分配一个即可上网了。

(二) 通过光纤专线上网配置

网络拓扑如图所示：路由器以太网口 ETH2/0 连接到电信光纤，网络地址为 142.1.1.0/30，以太网口 ETH3/0 连接到网络光纤，网络地址为 162.1.1.0/30，以太网口 ETH1/0 连接到网吧局域网，

182

私网 IP 网络地址为 192.168.1.0/24。



网络拓扑

1. 华为 2811 路由器的配置

用反转线将设备的 Console 口与主机的 COM1 相连接。



连接到华为 2811 路由器

打开 Windows 系统自带的“超级终端”，并在名称对话框中输入会话名称后按确定。



打开超级终端

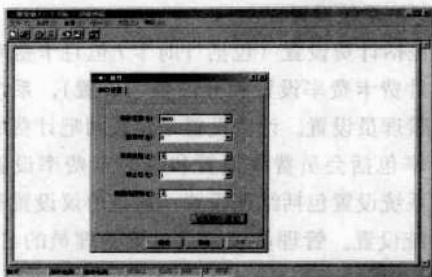
在下面的对话框中选择 COM1。



选择连接的串口

第九章 网吧局域网组建实战

在下面的对话框中选择“还原默认值”。



配置连接参数

接下就可以看到华为路由器的命令操作窗口。



华为路由器的操作窗口

在路由器中配置以下命令：

```
sysname Quidway
#
clock timezone gmt+08:00 add 08:00:00
#
cpu-usage cycle 1min
#
connection-limit disable
connection-limit default action deny
connection-limit default amount upper-limit 50
lower-limit 20
#
radius scheme system
#
domain system
#
detect-group 1
detect-list 1 ip address 140.1.1.2
#
detect-group 2
detect-list 1 ip address 162.1.1.2
#
```

```
acl number 2000
rule 0 permit
#
acl number 3001
rule 0 permit ip source 192.168.1.0 0.0.0.254
内部 pc 机偶数地址
acl number 3002
rule 0 permit ip source 192.168.1.1 0.0.0.254
内部 pc 机奇数地址
#
interface Aux0
async mode flow
#
interface Ethernet1/0
ip address 192.168.1.1 255.255.255.0
ip policy route-policy routeloadshare
从局域网收到的数据通过策略路由转发数据
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface Ethernet1/3
#
interface Ethernet1/4
#
interface Ethernet1/5
#
interface Ethernet1/6
#
interface Ethernet1/7
#
interface Ethernet1/8
#
interface Ethernet2/0
ip address 140.1.1.1 255.255.255.252
nat outbound 2000
#
interface Ethernet3/0
```



```
ip address 162.1.1.1 255.255.255.252
nat outbound 2000
#
interface NULL0
#
route-policy routeloadshare permit node 1
if-match acl 3001          局域网 pc 机地址是
偶数的从 ethernet2/0 转发
apply ip-address next-hop 140.1.1.2
route-policy routeloadshare permit node 2
if-match acl 3002          局域网 pc 机地址是
奇数的从 ethernet3/0 转发
apply ip-address next-hop 162.1.1.2
#
ip route-static 0.0.0.0 0.0.0.0 140.1.1.2 preference 60
detect-group 1
ip route-static 0.0.0.0 0.0.0.0 162.1.1.2 preference 60
detect-group 2
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
```

2. 服务器以及客户机上网的配置

服务器以及客户机的设置如下：IP 设置为 192.168.1.x，各机器不要重复即可，子网掩码 255.255.255.0，网关设成路由器的 LAN 口 IP 地址，即 192.168.1.1，DNS 根据当地 ISP 的服务器地址而定。

9.6.4 计费服务管理系统

如今大型、中型网吧的规模基本都在 300 台机器以上，如此庞大的机器数量和每天成千上万人的客户流量给网吧带来了可观的效益，在形成规模的网吧中财务管理已不再像几十台小型店里的那么简单了，尤其网吧都采用电脑计费系统，那么作为网吧财务管理出纳环节中的“网吧计费服务管理系统”既是收银所采用的工具又是财务统计的工具，它的重要性可想而知。下面我们以后在网吧在使用得较多的美萍计费管理专家 v8.7 版为例，为大家讲讲它的使用。

1. 名词解释和重要说明

(1) 系统设置：

包括计费设置（包括计时卡 / 包月卡费率设置，计费卡费率设置和分段费率设置），系统设置和管理员设置。计费设置是设置网吧计费的基本费率包括会员费率设置和临时卡费率设置两种。系统设置包括结账设置，通讯协议设置和其他系统设置。管理员设置是设置管理员的名称、密码和权限。

(2) 最低消费：

就是所谓的开机费用。

最小收费：收费的最小单位。

(3) 通宵计费：

在此时间段内上机，费用不是按照费率计费的，而是按照此时间段内的费用总额计费。如通宵计费设置为从 22 点，持续 8 小时，会员价为 8 元，普通价为 10 元，那么在此时段内上机不论有没有达到 8 小时，会员卡支付 8 元，临时卡支付 10 元。

(4) 星期费率设置：

即一个星期里的打折设置。例如星期一按照基本费率的 90% 收取费用，即打 9 折。

(5) 从属计算机设置：

即设置某台电脑的上机费率。如果某台电脑没有从属于某个费率，那么这台电脑就按照标准费率计费。

(6) 批量添加：

即成批的添加会员卡。但批量添加的会员卡不能正常上机，必须被激活之后才能正常上机。

(7) 远程操控：

操作控制所选的客户端电脑。

(8) 锁屏：

将客户端的电脑屏幕锁定，即客户端电脑不能进行任何操作。

(9) 解锁：

将锁屏的客户端电脑恢复到正常使用状态。

(10) 快速通道：

用户可以使用相应操作命令进行相关的操作。

命令如下：

1) 输入电脑名称上机或下机，命令是：\电脑

第九章 网吧局域网组建实战

名，例如：\001。

2) 激活临时卡，命令格式是：/ 临时卡号，例如：/L123 或 /123。

3) 显示会员卡详细信息并修改会员信息，命令格式是：* 会员卡号，例如：*111。

4) 给计费会员卡加钱，命令格式是：+ 会员卡号 金额，例如：+111 20。

5) 给计时会员卡加机时，命令格式是：\ 会员卡号 机时，例如：\222 120。

6) 给包月会员卡加月数，命令格式是：// 会员卡号 月数，例如：//333 2。

7) 锁定指定的电脑，命令格式是：++ 电脑名 例如：++001。

8) 关闭指定的电脑，命令格式是：- 电脑名 例如：-001。

9) 锁定所有电脑，命令是：LOCKALL。

10) 关闭所有电脑，命令是：CLOSEALL。

刷卡设备说明：

计费专家可直接支持条码卡、磁卡、射频 IC 卡等刷卡设备，不需要安装任何驱动程序，因为这些读卡设备都是基于模拟键盘输入的。对普通 IC 卡，因为不同厂家的 IC 卡设备有不同的驱动程序，所以需要编写特别的驱动才可以使用。

购置卡的建议：可以在当地的制卡公司一次制作一批卡（一张卡 1 元左右），可以选择磁卡或者条码卡。磁卡刷卡器和条码卡阅读器一般都在 300 元左右。然后利用软件中的批量生成卡的功能来生成会员卡。临时卡也可以按照上面方法制作一批。普通 IC 卡的读卡、写卡设备要按照不同的驱动，不建议购买。

小票打印机购买说明：

安装程序中自带 pos58 的小票打印驱动程序，只要 POS58 系列的热敏小票打印机都可正常使用。

热敏小票打印机（58mm）价格一般在 1000 元左右，各地价格有所不同，一卷热敏打印纸价格在 1.5 元左右，价格低廉，不需要其他耗材，速度快，故障率低，推荐大家使用。

2. 软件常用操作

(1) 上机：双击所选电脑或选中电脑按回车键，

弹出上机窗口后，填写相关的信息，然后点击确定按钮或按 F5 键上机。

(2) 下机：双击所选电脑或选中电脑按回车键，弹出下机窗口后，填写相关的信息，然后点击确定按钮或按 F5 键结账下机。

(3) 购买商品：如果将购买商品费用指定给上机电脑，则先选中电脑，然后点击销售商品按钮或点击鼠标右键选择销售商品选项，弹出销售商品窗口后，进行商品购买。

3. 日常运行步骤

STEP 1 双击图标打开本系统；

STEP 2 输入正确的用户名及密码进行登录；

STEP 3 登记模块：来宾登记→预订管理；

STEP 4 登记模块：来宾登记→顾客开单；

STEP 5 点单模块：点单消费→增加消费；

STEP 6 收银模块：收银结账→宾客结账（确认或询问客人是否是为本店会员）；

STEP 7 查询模块：查询来宾信息、收银明细、打印营业情况日、月报表、统计分析营业收入及宾流量等；

STEP 8 会员管理模块：管理会员的基本信息、消费信息；

STEP 9 维护系统→数据备份；

STEP 10 维护系统→系统设置。

4. 各功能模块操作方法

系统主界面：



红色图标表示此电脑无法通讯即不能和客户端连接。

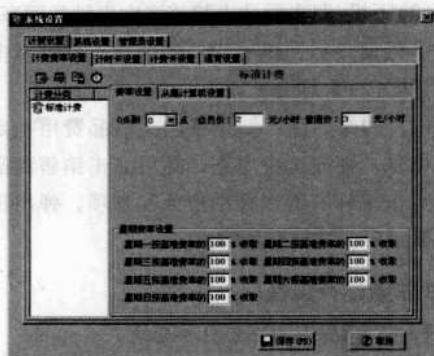
“锁”图标表示此电脑通讯正常但是被锁屏。

“电脑”图标表示此电脑通讯正常且正处于使用状态。



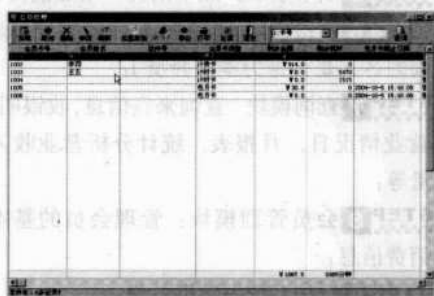
(1) 系统设置

在系统设置里设置上机的费率；



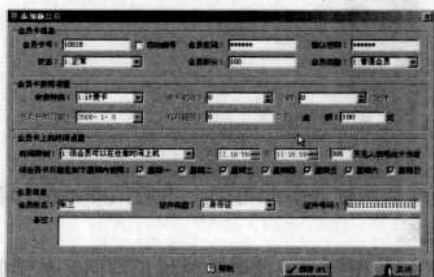
设置上机费率

会员管理（点击系统主窗口里的会员管理按钮）；



会员管理

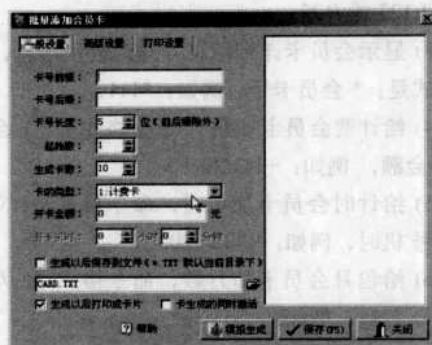
添加新会员（即点击会员管理界面里的添加按钮）：在此窗口中填写新会员的相关信息及此会员卡的其他设置，然后点击保存按钮或按 F5 键进行保存。



添加新会员

批量添加会员（即点击会员管理窗口中的批量添加按钮）：在此窗口中填写新会员的相关信息

及此会员卡的其他设置，然后点击保存按钮或按 F5 键进行保存。



批量添加会员

在此窗口中填写相关信息，如在一般设置里设置卡号的长度，生成卡数，起始数，开卡金额，开卡机等，在高级设置里设置这些卡的使用时间的限制。您可以在填写完相关信息后，点击模拟生成按钮，此时在右边的编辑框内生成了相应的卡号及密码，但是这些卡号和密码并没有保存，只是模拟产生的卡号和密码，如果您看后要保存，点击保存按钮或按 F5 键即可。会员卡生成还不能使用（此时的状态为禁用），要被激活后才能使用，此时就要在会员管理界面里，先选择会员卡，然后点击激活卡按钮。

(2) 加钱、加时、加月

在会员管理界面里选择要加钱（加时、加月）的计费（计时、包月）会员卡然后双击或按鼠标右键选择加钱（加时、加月）选项或点击加钱（加时、加月）按钮进行加钱（加时、加月）。

(3) 修改

在会员管理界面里选择要修改信息的会员卡，然后点击修改按钮或按鼠标右键选择修改选项。

(4) 过滤

在会员管理界面里显示出已过期的会员卡信息或所有包月卡的信息或金额少于 0.5 元的计费会员卡或机时少于 10 分钟的计时会员卡等。如果您看过后要显示所有的会员的记录，您点击刷新按钮或按鼠标右键选择刷新选项即可。

(5) 查询

在会员管理界面里，先选择下拉列表框里的

第九章 网吧局域网组建实战

查询关键字（即按什么查询），然后在文本框里填写查询的内容（可以是要查询内容的一部分即模糊查询），然后再点击查询按钮进行查询。

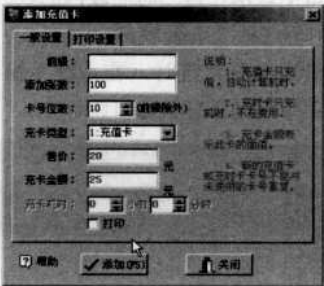
充值卡管理



充值卡管理界面

添加充值卡

添加充值卡的窗口里填写相关信息，如添加张数、卡号位数、充卡类型、售价、充卡金额等。最后点击添加按钮或按 F5 键保存生成的充值卡。



添加充值卡

出售充值卡

在下拉列表框里，先选择只显示未出售的充值卡选项，然后在数据列表里选择要出售的充值卡，然后再点击出售按钮即可。

5. 查询

如果您要查询未出售的充值卡，先选择下拉列表框里选择只显示未出售的充值卡选项，然后在文本框里输入充值卡的卡号（可以使卡号的一部分即模糊查询），然后再点击查询按钮。如果您要查询已出售的充值卡，先选择下拉列表框里选择只显示已出售的充值卡选项，然后在文本框里输入充值卡的卡号（可以使卡号的一部分即模糊查询），然后再点击查询按钮。

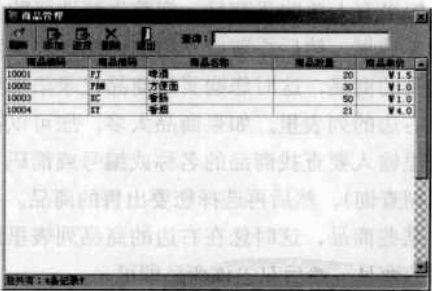
临时卡管理



临时卡管理界面

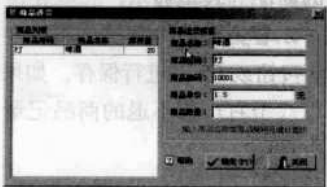
查询已激活的临时卡记录，先选择已激活的临时卡记录选项，然后在下拉列表里选择查询关键字（即按照什么查询），然后在文本框里输入查询内容（可以是查询内容的一部分即模糊查询），最后点击查询按钮。查询临时卡上机记录，先选择临时卡上机记录选项，然后在下拉列表里选择查询关键字（即按照什么查询），然后在文本框里输入查询内容（可以是查询内容的一部分即模糊查询），最后点击查询按钮。查询之后，如要显示所有的已经激活的临时卡记录或临时卡上机记录，点击刷新按钮即可。

6. 商品管理



商品管理界面

(1) 商品进货（在商品管理窗口里点击进货按钮）

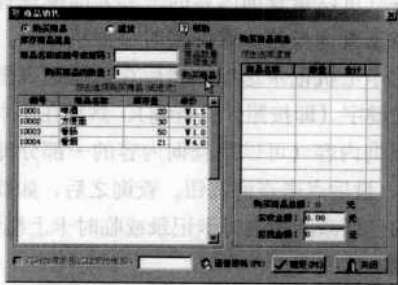


商品进货



在商品进货时先填写商品名称，然后按 Enter 键即回车键，商品简码自动产生在商品简码的文本框里，然后在填写商品编码，商品单价和商品数量，确认填写的信息没有错误后点击确定按钮或 F5 键进行保存。这时在窗口的左边添加了一条新记录。如果您要添加的商品名称在左边的商品列表里已经存在，那么您只要选择这条纪录，然后双击，这时在窗口的右边的商品名称，商品简码和商品编号已经填写好了，您只需要填写商品单价和商品数量即可（注意：您这时填写的商品单价要覆盖掉您以前商品的单价）。

(2) 商品销售（在系统主界面里点击销售商品即可）



商品销售

如果有人要购买商品，您首先要选择购买商品的单选框，然后在窗口左边的商品列表里双击要购买的商品，这时您购买的商品记录添加到了窗口右边的列表里。如果商品太多，您可以在文本框里输入要查找商品的名称或编号或简码（支持模糊查询），然后再选择您要出售的商品。如不想要某些商品，这时您在右边的商品列表里选择要退的商品，然后双击该商品即可。

如果有人要退货，您首先要选择退货的单选框，然后在窗口左边的商品列表里选择要退的商品记录，然后双击该记录，这时您要退的商品记录在右边的商品列表里显示，您就在窗口右边的商品总额可以看到要退的商品总额是多少，然后再点击确认按钮或 F5 键进行保存。如果又不想退货，您可以双击右边您不退的商品记录（操作与购买商品相同）。

7. 日常管理

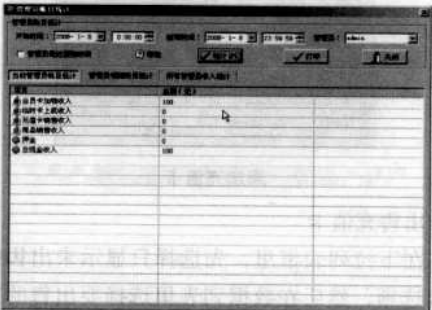
(1) 收入统计（在系统主窗口中选择日常管理菜单下的收入统计）



收入统计

收入统计是统计某个时间段内的各项收入。如果您要查询某个时间段内的收入，您先选择开始日期，再选择结束日期，然后再点击刷新按钮即可在窗口中显示在这一时间段内的收入统计（注意：合计中不包括欠款金额）

(2) 管理员账目统计（在系统主窗口中选择日常管理菜单下的管理员账目统计）

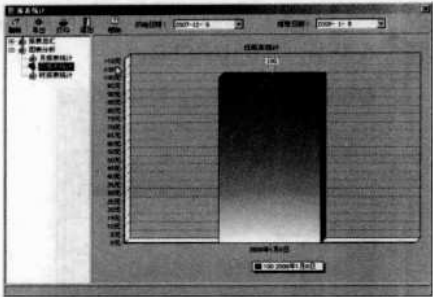


管理员账目统计

管理员账目统计是统计某个管理员在某一时间段内的现金收入。如果您要查询某个管理员在某个时间段内的现金收入，您先选择开始日期时间，再选择结束日期时间，然后再选择管理员名称，最后点击统计按钮或按 F5 键即可。在窗口中就显示出您所有查询的结果（注意：押金只有当前管理员有，而且押金不包括在总现金收入里）。

(3) 报表统计（在系统主窗口中选择日常管理菜单下的报表统计）

第九章 网吧局域网组建实战



报表统计

报表统计包括报表总汇和图表分析两大项。报表总汇包括临时卡上机统计、会员卡上机统计、充值卡使用统计和电脑上机统计。图表分析包括月报表统计、日报表统计和时报表统计。如果您要查询首先您要选择开始日期和结束日期，然后点击窗口左边相应的选项（例如月报表统计）或选择好窗口左边的选项后在点击刷新按钮即可（注意：时报表统计是按开始日期统计的）。

(4) 上机和结账

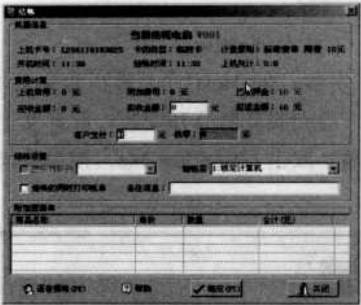
上机。如果要上机您只需要在系统主窗口中选择好电脑后双击此选项或按回车键即可。然后在上机窗口中填写相关信息，点击确定按钮或按 F5 键进行保存。



上机

结账。如果要结账您只需要在系统主窗口中选择好电脑后双击此选项或按回车键即可。如果您把产生的上机费和附加费转移到另一台电脑（这样就可以不产生任何费用），您就要选择转移费用选项。结账后下拉列表里是此电脑结账之后服务端对此客户端的操作，有锁定计算机，关闭计算

机，关闭所有程序等操作。填写完相关信息之后，您点击确定按钮或按 F5 键进行保存。



结账

9.6.5 CS服务器搭建

现在网吧越开越多，竞争也越来越激烈，每个网吧管理员都想提高网吧的竞争能力，本节就来谈谈一个网吧需要的额外服务。

CS 是时下依然热门的游戏，大多数在网吧玩 CS 的人数还是占半数以上的，要想留住这些 CS 人群，就需要为他们建立一个专用的 CS 服务器。

1. 硬件要求

服务器的最低硬件配置为 P3 500MHz，内存 256MB 以上，建议还是用 P4 以上配置，这样，可以在一台服务器上多建几个 CS 服务器。

2. 线路要求

线路当然是越快越好，我们把 CS 服务器架在主干交换机上，尽量提高 Ping 的速度，一般来讲，服务器进满 28 个人之后 Ping 值在 20ms 之内，多了就会死机。

3. 服务器的架设

我们以 GameHost 架设 CS 服务器为例，GameHost 的优势在于：

- 1) 可以把服务转到后台去，这样更加有利于 cs 服务器的稳定性（要在 windowserver 上）；
- 2) 你可以随时管理 cs 服务器，只要在机器上安装客户端；
- 3) 可以多人管理权限可以不同，一台服务器上安装了 GameHost，就可以开数个 cs 服务器（只



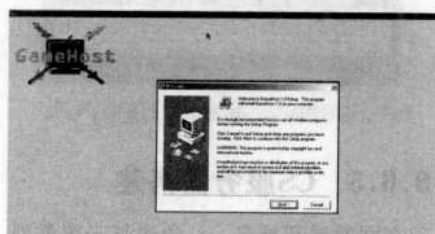
要你配置够用)；

4) 自己可以计划任务，占资源非常小。

架设过程：

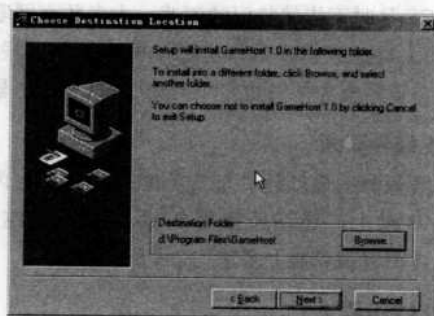
1) 下载 GameHost；

2) 安装 GameHost（分客户端和服务端，建议客户端和服务端分开安装，服务器上只安装服务器端）双击 GameHost.exe，接受协议，然后下一步。



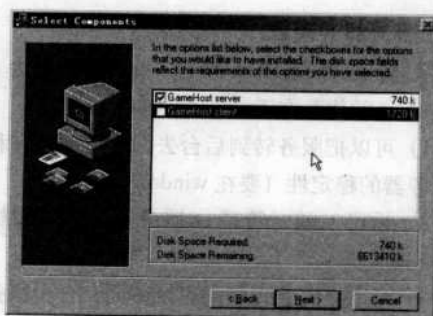
GameHost的安装

3) 选择安装路径；



选择安装路径

4) 然后选择安装内容，有两个选项，第一个是服务器端，第二个客户端也可以叫控制端，建议只安装服务器端；



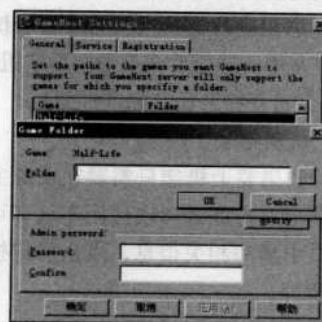
选择安装内容

5) 然后下一步，直到出现下面的对话框，这里选择游戏类型，双击 Half-life。



选择游戏类型

6) 然后在弹出的对话框里，找到你的 cs 服务器程序放置的文加夹即可（不用指定 hlds.exe）。



指定服务器程序所在的文件夹

7) 选择完以后，输入 cs 服务器远程控制密码（注意这里的密码不是 op 密码，而是 GameHost 服务器端控制密码，这个密码是新设置的，一定要记住这个密码，这样以后用 Gamehost 客户端登录要使用这个密码的）。



输入远程管理密码

第九章 网吧局域网组建实战

8) 最后单击 Registration 标签, 输入注册码 (没有注册码只能用 30 天)。

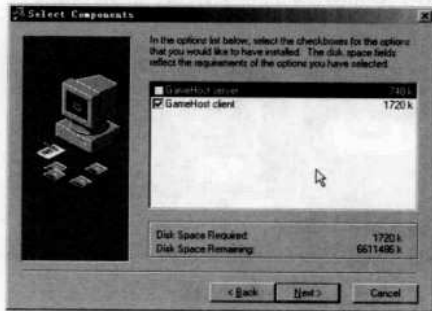


注册软件

至此服务器端已经设置完毕, 下面开始设置客户端, 也就是控制端。

4. 客户端的安装与配置

客户端很好安装, 和服务器端安装一样不再赘述, 只是选择 Gamehost client 点击下一步就可以。



安装客户端

安装后运行 Game Host console, 接下来连接服务器, 配置 cs 服务器,



连接到服务器

建立服务器连接后,



与服务器建立连接

下面详细说一下配置:

1) 下面开始远程配置 cs 服务器, 选择游戏类型。



选择游戏类型

2) 选择服务器的 IP 地址和端口。



选择服务器的IP地址和端口

3) 配置服务器启动参数。



配置服务器启动参数

4) 远程配置服务器完毕后。



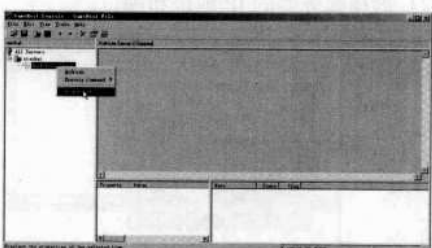
服务器配置成功

5) 启动服务器。



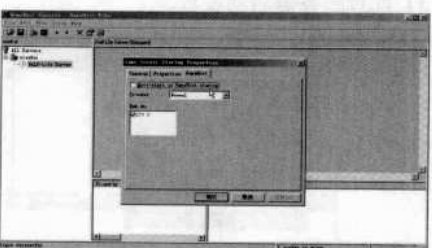
启动服务器

6) 服务器启动、定时任务等设置。



服务器启动、定时任务设置

7) 选择由哪个CPU处理服务。



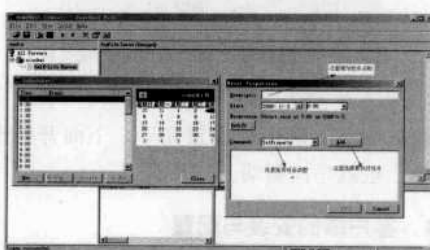
选择处理的CPU

8) 选择服务器运行的模式。



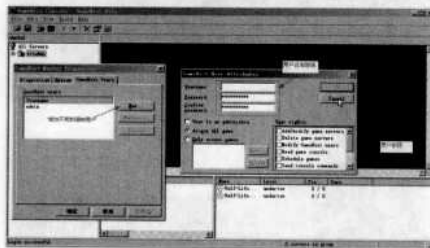
选择服务器运行的模式

9) 配置定时任务。



配置定时任务

10) Gamehost 管理员添加、权限设置。



用户管理

9.6.6 电影音乐服务器搭建

为了吸引更多的人来上网，一些网吧开始架设电影服务器。电影服务器的架设不是很简单地设置共享硬盘，然后拷些电影就OK了。为了最大化地利用网吧资源，顺便把电影服务器设为Web服务器。

硬件配置：

建议配置为P4 2.6 GHz、1G内存、200GB以上硬盘。

软件配置：

推荐服务器版本 Win2003EE SP1 或者 Win2000 高服版 + SP4，IIS6.0 或更高，电影服务器版

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第九章 网吧局域网组建实战

本为《FJ51758 网吧电影系统 V4.0》，视频加速用流媒体 rs905-1159-win32。

安装过程：

1.安装IIS 6.0

双击控制面板→添加或删除程序→添加/删除 Windows 组件→应用程序服务器→Internet 信息服务 (IIS)→确定并安装，



安装IIS 6.0

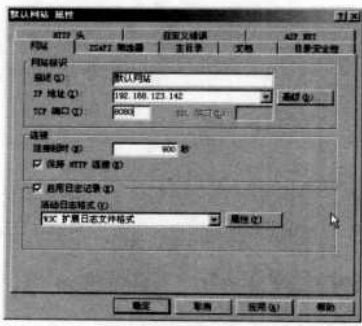
2.建立网站

打开 IIS 管理器→右击网站→新建→网站→打开向导→在网站描述里输入网站内容，



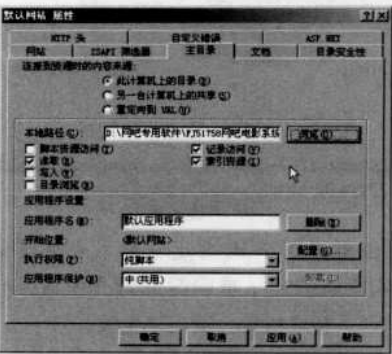
建立网站

网站 IP 为本机 IP，端口为 8080（默认为 80），



设置网站

另外，不能使用默认路径，所以要更改一下：把 FJ51758 网吧电影系统 V4.0 放进去，权限为前 3 项，然后点”完成”。



将电影系统放入IIS

3.其它设置

打开 Web 服务扩展→允许第 3 项（即 Active Server Pages）；右击你建立的网站属性→主目录→配置→选项→启用父路径。再选文档→添加→键入 index. asp 上移到最上→确定。

4.浏览及管理电影服务器

打开 IE — 键入你的服务器 IP（如：192.168.123.142:8080/index.asp），即可浏览网站，



测试电影服务器

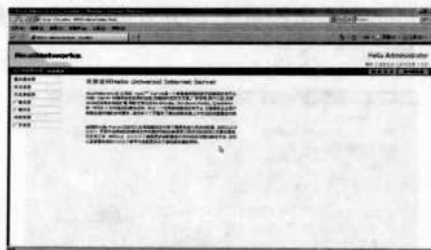
再打开后台管理（如：192.168.123.142:8080/admin.asp），键入说明里的用户名和密码即可管理，如：添加电影及会员等服务。

5.安装流媒体软件

打开流媒体 rs905 — 下一步，输入管理员账号及密码→在 HTTP 项键入 8075 →下一步到完成。打开 Helix Server 服务—再打开 Helix Server Administrator →输入管理员及密码，

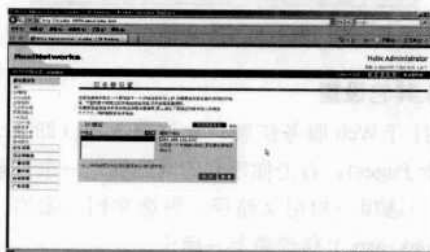


打开流媒体界面，



流媒体界面

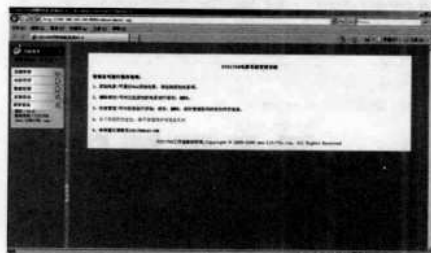
服务器设置→IP绑定→输入服务器IP（如192.168.123.142）→重启服务器并生效。打开配置加载点→新增加载，重启并生效。



配置流媒体软件

6. 添加电影

进入电影管理后台，



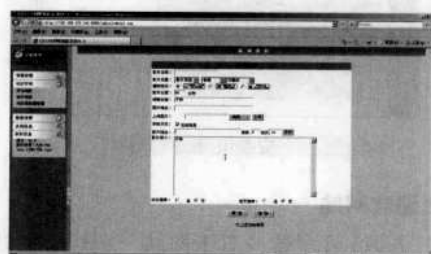
电影管理

电影管理→电影服务器管理→增加服务器，



增加电影服务器

添加电影，



增加电影

7. 测试电影



测试电影

至此，电影服务器就架设完毕了。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

管理维护篇

第十章 服务器搭建、配置与管理

第十一章 网络升级与优化实战

第十二章 服务器远程管理与维护

第十三章 局域网安全管理与维护



第十章 服务器搭建、配置与管理

本章主要讲解在 Windows 2000/XP/2003 环境下，如何在局域网和 Internet 提供各种网络服务，从搭建 FTP 服务器、邮件服务器、流媒体服务器等方面展开，为入门级的网络管理员提供完整的解决方案，只要按照图书中的步骤操作，就能轻松搭建自己的服务器。

10.1 用IIS6.0搭建Web服务器

IIS6.0 是 Windows 系列操作系统中最新的服务器平台，它能够迅速建立与部署网站及其应用程序的服务。IIS6.0 除了集成 ASP.NET 以外，还能提供自动检查服务器本身的各种状态的功能，如：网站状态、内存与访问状态等，并能适时对这些状态进行容错处理。此外，还可以让单一服务器架设比 IIS5.0 更多的站点。

10.1.1 什么是Web服务器

可匿名访问的 Web 服务器，就是无需用户名和密码就可以访问的网站，也就是网民平时接触最多的网站。

Web 也称为 WWW（World Wide Web，万维网），它最初是由设在日内瓦的欧洲核物理研究中心(CERN)的 Tim 和他的同事开发的。1993 年 1 月，NCSA（美国超级计算应用国家中心）就推出了第一个 Web 浏览器 Mosaic。完全可以这么说，Web 应用是因特网服务里当之无愧的王者！不信？你看现在哪些因特网服务不可以借助 Web 浏览器来

完成？很多邮件服务器都支持 Web Mail 方式，绝大多数 FTP 服务器支持使用 Web 浏览器来列目录、下载文件等。

和 Web 关系最紧密的一个概念就是 HTTP（超文本传输协议）。在因特网上，使用 Web 浏览器时，HTTP 协议负责传输 Web 页面，定义 Web 服务器和浏览器之间的通信。在一个典型的 HTTP 会话中，Web 浏览器初始化与服务器的连接，并请求某文档或者服务，然后 Web 服务器响应这种请求并传输所需文档。

在 Windows Server 2003 中使用 IIS 6.0 架设匿名可访问网站，实在是件轻而易举的事情。下面来看看架设过程。

10.1.2 安装IIS6.0及Web服务组件

因为在 Windows Server 2003 中，默认状态下是不安装 IIS 6.0 的，所以需要先安装 IIS 6.0。依次点击“开始→设置→控制面板→添加或删除程序”菜单。在弹出的“添加/删除 Windows 程序”窗口中点击左侧导航栏中的“添加/删除 Windows 组件”。接着在弹出的“Windows 组件向

第十章 服务器搭建、配置与管理

导”窗口中，单击选中“应用程序服务器”项后，单击下方的“详细信息”按钮。

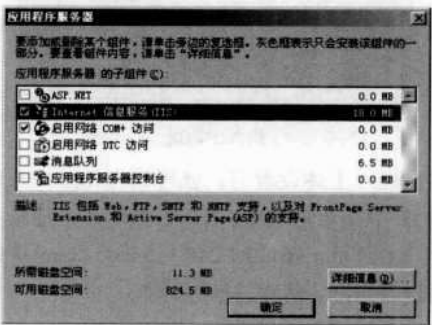


选中“应用程序服务器”

注意

应用程序服务器大多数都是在 Client/Server（客户机/服务器）网络体系中存在的。它利用客户端和服务端应用程序，由客户机请求，并将请求发送到应用程序服务器中，这时应用程序服务器就代替客户机执行任务，并把所执行任务的结果的信息返回给客户端。

在随即弹出的“应用程序服务器”子组件窗口中单击“Internet 信息服务 (IIS)”，然后单击“详细信息”。



单击“Internet 信息服务(IIS)”

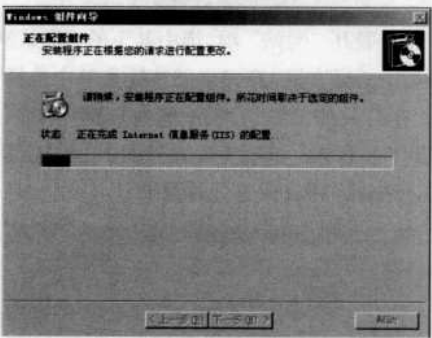
在打开的“Internet 信息服务 (IIS)”组件列表窗口，点击选择“万维网服务”组件后，单击“确定”按钮。



注意

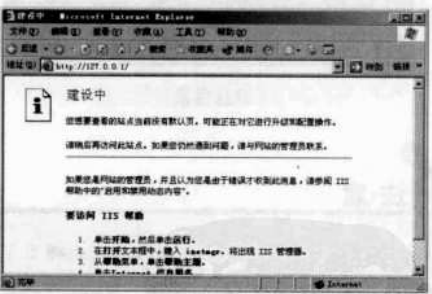
在选中“万维网服务”组件后，在列表中会自动选中一些相应的辅助组件，这些默认选中项，不要点击取消其选中状态。

在返回“Windows 组件向导”后，单击“下一步”按钮就可以开始 IIS6.0 的 Web 服务组件的安装了。



开始安装

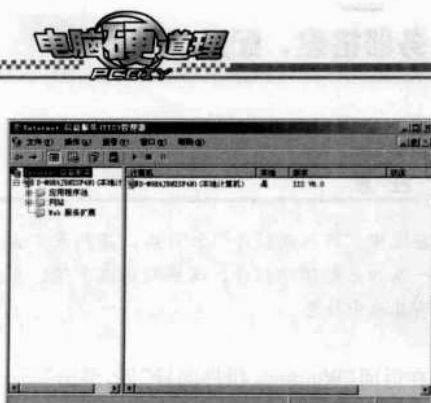
安装完成后退出“Windows 组件向导”。如果想检查一下 IIS6.0 是否运行正常，只需打开一个 IE 窗口，在地址栏中输入“http://127.0.0.1”并回车，如果看到如下页面信息，则表示 IIS 正常。



检查IIS6.0是否正常

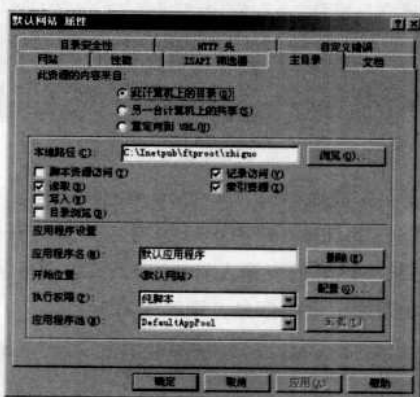
10.1.3 配置Web组件

依次点击“开始→管理工具→控制面板→管理工具→ Internet 信息服务 (IIS) 管理器”，打开相应的管理窗口。



打开IIS管理器窗口

点击展开“网站”项，选中其下的“默认网站”项并点击鼠标右键，在弹出的快捷菜单中选择“属性”。在打开的“默认网站 属性”窗口中，点击切换到“主目录”选项卡设置界面中，点击“浏览”按钮，选择好存放有主页的目录。



设置目录



注意

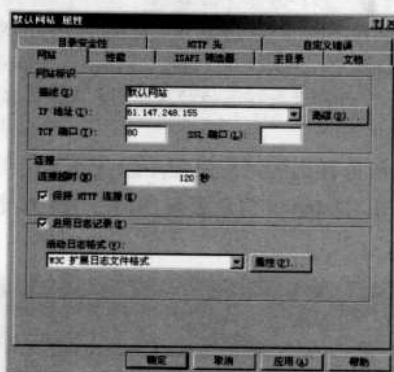
基于安全考虑，不要在C盘或其它盘根目录下创建Web内容目录。

接着根据网站中设计的首页文件名不同，有可能还需要点击切换到“文档”选项卡设置界面，点击“添加”按钮，在弹出的对话框中添加相应的首页名和后缀名。



设置首页名和后缀名

最后点击切换到“网站”选项卡设置界面，在IP地址框中输入要指定给此Web站点的IP地址（如果仅想在局域网中使用，那么输入当前计算机的内网IP地址即可）。



输入IP地址

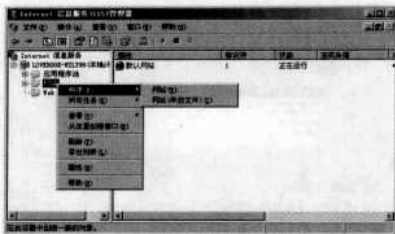
在经过上述设置后，就可以在任意一台计算机的IE中使用匿名方式输入“http://IP地址+首页名”（如http://61.147.248.155/index.html）这样的网址对架设的网站进行访问了。

10.1.4 建立多个网站

如果需要在服务器中建立多个网站，那么方法有很多种。但是在要求不高的情况下，建议使用在IIS中新建网站的方法来实现。

在IIS窗口中，选中“网站”项并右键单击鼠标，在弹出的快捷菜单中选择“新建→网站”项。

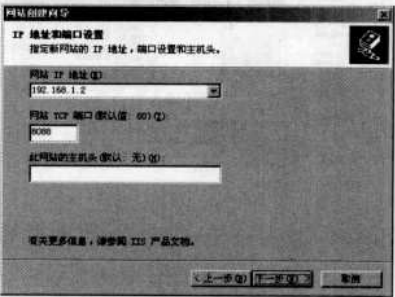
第十章 服务器搭建、配置与管理



新建网站

在接着出现的网站创建向导欢迎画面中，单击“下一步”按钮继续。在出现的“网站描述”对话框中，输入一个容易让网管维护时识别的名称。如财务科的首位拼音组合“cwk”。

接着在“IP 地址和端口设置”对话框中，指定网站访问 IP 地址及相应的端口号。在多个网站的情况下，我们可以通过设置不同的端口号来访问不同的网站。



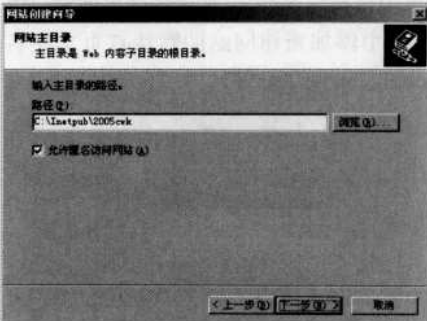
设置端口

接下来在“网站主目录”对话框中需要指定新建网站的目录路径，点击“浏览”按钮。在弹出的“浏览文件夹”对话框中，如果没有事先创建好网站目录，那么在选中主目录后再点击“新建文件夹”按钮，新建一个对应的网站目录。如下图所示已经事先建立了网站目录，这里只需直接选中目录并单击“确定”按钮即可。



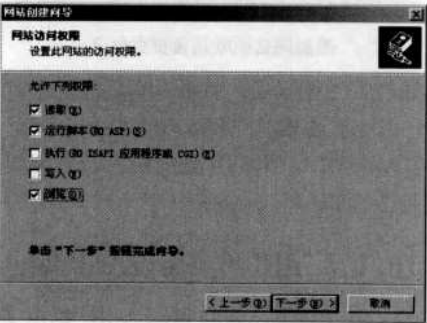
设置路径

接着将目录路径添加好。



添加路径

在接着出现的“网站访问权限”对话框中，可以根据局域网中的具体情况设置访问权限。



设置访问权限

最后，在完成界面中点击“完成”按钮即可结束新网站的创建。

在返回到 IIS 窗口后，可以看到在网站下新建的“CWK”子网站。点击工具栏上的“开始”、“停止”、“暂停”三个按钮，可以快速进入相应的状态。

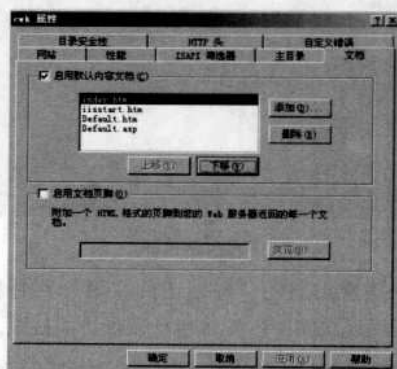


新建的“CWK”子网站

接着，将设计的网站内容全部拷贝到新建的网站目录中。复制完毕后，在 IIS 窗口中，选中



新建的 CWK 网站并单击鼠标右键，在弹出的快捷菜单中选择“属性”。在随即弹出的窗口中，在“文档”中添加新建网站的默认首页文件名，如 index.htm、index.asp 等。



添加网站的默认首页文件名

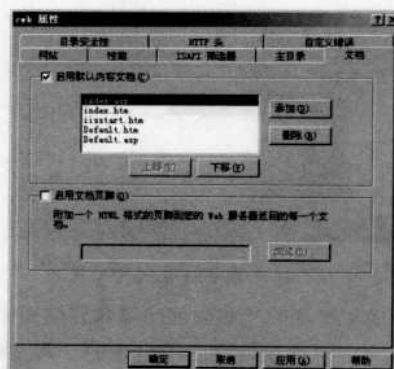
经过上述设置后，就可以在任意一台计算机的 IE 中，通过输入“http://IP 地址: 8088”（如 http://192.168.1.2: 8088）这样的网址对架设的网站进行访问了。

10.1.5 用 IIS6.0 架设 ASP 网站

Internet 上的网页不仅可以为用户提供文字和图片的浏览，还可以通过表单与用户进行互动，通过后台程序在服务器之间传递数据。如果想实现这些互动功能，就需要提供某些服务，使客户端能够识别用户发出的指令，并把指令传递给服务器端，同时使服务器能够处理客户端传送过来的数据。Microsoft Active Server Page (ASP) 就是用来实现这些功能的。

要架设 ASP 网站，在 IIS6.0 中是很容易的。首先，我们需要在 IIS 窗口中选中“网站”并单击鼠标右键，在弹出的快捷菜单中选择“新建→网站”菜单项，在新建一个网站（使用的端口为 8088）后，将设计的 ASP 网站文件复制到对应的目录中。

接着在 IIS 窗口中，选中这个网站并单击鼠标右键，在弹出的快捷菜单中请选择“属性”。在接着打开的窗口中，在“文档”选项卡设置界面中，添加 index.asp 首页文件，接着点击“上移”按钮将其移动到最上方。



上移“首页文件”

稍后，在 IIS 窗口中，选中左侧的“Web 服务扩展”项，接着在右侧选中 Active Server Pages 项并单击中间的“允许”按钮。



设置为“允许”

最后，就可以通过“http://192.168.1.2:8088”这样的网址来访问新建的 ASP 网站了。

10.1.6 用 IIS6.0 架设 ASP.net 网站

ASP.net 不仅仅是 ASP 的下一代产品，更重要的是它为 Internet 创建新的网络应用提供了全新的编程模型。ASP.net 是统一的 Web 应用程序平台，它提供了为建立和部署企业级 Web 程序程序所必需的服务。ASP.net 为能够面向任何浏览器或设备的更安全的、更强的可升级性和更稳定的应用程序提供了新的编辑模型和基础结构。ASP.net 是 Microsoft.net Framework 的一部分，是一种可以在高度分布的 Internet 环境中简化应用程序开发的计算环境。

第十章 服务器搭建、配置与管理

1. 安装ASP.net

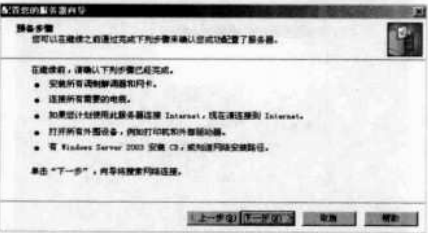
安装 ASP.net 既可以在“添加 / 删除程序”中进行，也可以通过极为方便的“配置您的服务器”向导中进行。使用配置服务器向导安装 ASP.net 的过程如下：

首先，依次点击“开始→管理工具→管理您的服务器”菜单。在接着弹出的界面中，点击“添加或删除角色”超级链接。



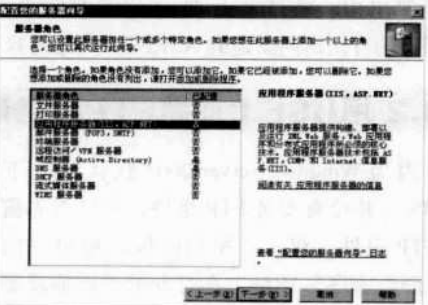
添加或删除角色

接着我们需要根据提示做好相应的准备。



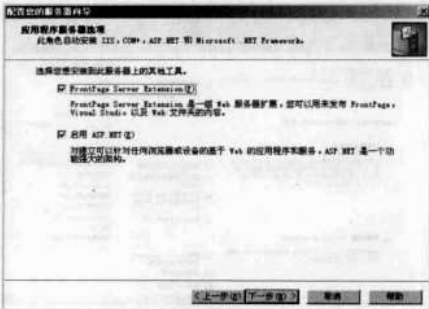
按提示做好准备

接下来，在“服务器角色”对话框中选择“应用程序服务器 (IIS,ASP.net)”项后，单击“下一步”按钮继续。



选择“应用程序服务器”项

在接着的“应用程序服务器选项”对话框中，点击勾选其中的两个选项。



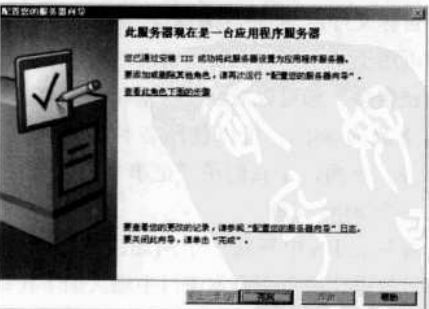
选中以上两项

在“选择总结”对话框中，可以看到即将执行的操作列表。



即将执行的操作

现在，将 Windows Server 2003 的安装光盘插入光驱，在单击“下一步”按钮后。在安装完成时，系统会打开配置完成对话框，此时单击“完成”按钮。



完成配置

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

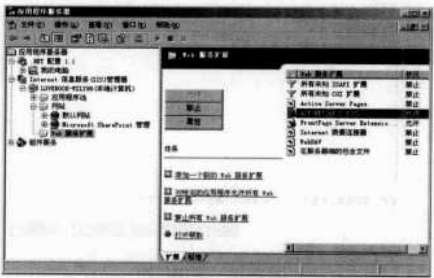


在返回“管理您的服务器”界面后，点击“管理此应用程序服务器”超级连接。



点击“管理此应用程序服务器”

在接着弹出的“应用程序服务器”窗口中，选中“Internet 信息服务 (IIS) 管理器”、“本地计算机”、“Web 服务扩展”项，接着在右侧选中“ASP.NET V1.1.4322”项，然后点击中间的“允许”按钮。



设置为“允许”

2. 网站架设

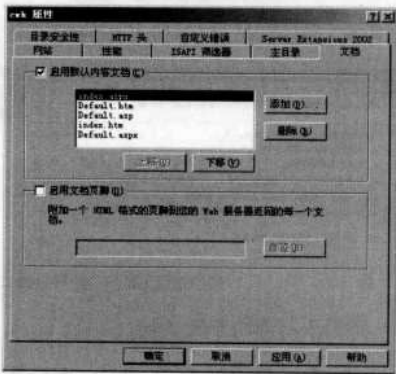
ASP.net的网站都是带.aspx 后缀名的文件，当浏览者请求浏览.aspx 资源时，ASP.net 运行库分析目标文件后，会将其编译成一个.NET 框架类。此类可用于动态处理传入的请求。编写.aspx 文件的方法很多，如可以直接将现有的 HTML 文件后缀名更改为.aspx，可以使用各种工具创建.aspx 文件等。下面，让我们用“记事本”工具来简单编写一个.aspx 文件。

首先在 IIS 中新建一个网站，其访问端口为 8088。接着，请在记事本窗口中输入如下代码：

```
<html>
<body>
<center>
<form action=" 123.aspx" method=" post" >
```

```
<h3> 关键字 <input id=" key" type=" text"
>
类别: <select id=" category" size=1>
<option> 财务科 </option>
<option> 企划科 </option>
<option> 资料室 </option>
</select>
<input type=submit value=" 查找" >
<h3>
</form>
</denter>
</body>
</html>
```

稍后，在 IIS 中新建的网站目录中，将这个文本文件的后缀名重命名为“index.aspx”。接下来，在 IIS 窗口中，选中新建的网站并进入其属性窗口，在“文档”选项卡设置界面中，添加 index.aspx 文件。



添加index.aspx文件

在经过上述设置后，就可以在任一局域网的计算机中，通过输入“http://192.168.1.2:8088”并回车的方法访问新建的 ASP.NET 网站内容了。

10.2 用IIS6.0搭建FTP服务器

因为 Windows Server 2003 默认状态下，安装 IIS 时并没有安装 FTP 组件，所以首先需要添加 FTP 组件。双击“控制面板”窗口中的“添加 / 删除程序”图标，在打开的“添加或删除程序”对话框中，单击左侧导航栏中的“添加 / 删除 Windows 组件”按钮，在接着弹出的“Windows

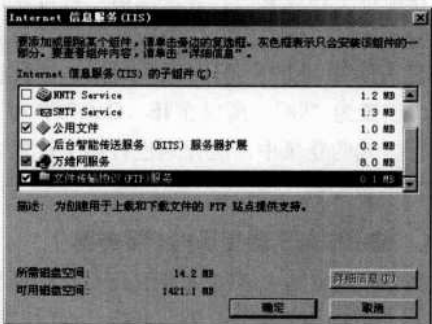
第十章 服务器搭建、配置与管理

组件向导”对话框中，选中并双击“应用程序服务器”项，然后在弹出的对话框中单击勾选“Internet 信息服务 (IIS)”。



勾选“Internet 信息服务 (IIS)”

接着，单击“详细信息”按钮，在弹出的对话框中将右侧的滚动条拖动至最下方，然后单击勾选“文件传输协议 (FTP) 服务”。



勾选“文件传输协议服务”

单击两次“确定”按钮后，再单击“下一步”按钮，即可开始从 Windows Server 2003 安装光盘复制所需文件至系统中，直至完成 FTP 组件的安装。

10.2.1 设置默认目录

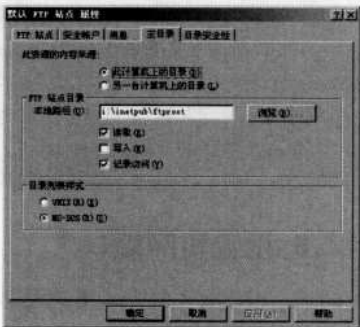
“默认目录”就是当 FTP 客户端用户登录 FTP 服务器时，默认访问的根目录，一般情况下，应当将资料放在 FTP 服务器的该目录中，以供网友下载。



默认目录可以是任一分区下的目录，也可以直接是整个分区。IIS 默认的 FTP 服务器主目录是安装系统的磁盘分区中的“inetpub\ftproot”目录。

依次单击“开始→设置→控制面板→管理工具→Internet 服务管理器”菜单项，在打开的“Internet 信息服务 (IIS) 管理器”对话框中，用鼠标右键单击“默认 FTP 站点”，然后在弹出的快捷菜单中选择“属性”命令。

在快捷菜单中，可以通过单击“启动”、“停止”或“暂停”菜单项来控制 FTP 服务器的运行或停止。在随后弹出的“默认 FTP 站点属性”对话框中，单击切换到“主目录”标签页。



切换到“主目录”标签页

接着，将“本地路径”改成指定的 FTP 服务器默认目录位置即可，如“i:\inetpub\ftproot”。建议将访问方式只设置为“读取”，该设置是指他人访问 FTP 服务器时，只能读取或下载内容，但是不能对其进行删除或修改等操作。

10.2.2 设置FTP服务器的IP地址

为了让别人能够访问 FTP 服务器，就必须为 FTP 服务器指定一个 IP 地址。在“默认 FTP 站点属性”对话框中，单击切换到“FTP 站点”标签页，然后单击“IP 地址”项右侧的下拉箭头，从弹出的 IP 地址下拉列表中选择符合要求的 IP 地址（如“192.168.1.13”）。



设置IP地址

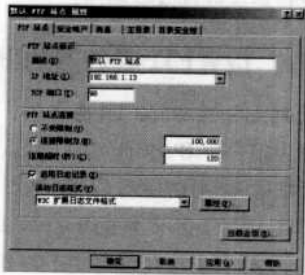
如果选择“全部未分配”项，那么无论使用哪个IP地址来访问FTP服务器，只要该IP地址属于它，就一定可以访问到该FTP服务器。



“描述”项的设置并不会影响到FTP客户端的访问，而是用来标识个人和组织身份的。其主要是用于这样的场合：本地服务器上安装多个FTP服务器（也就是虚拟站点），这样将会在“Internet 信息服务（IIS）管理器”对话框的左侧树状结构中显示不同的FTP服务器名，而不是千篇一律的“默认FTP站点”。

10.2.3 设置访问端口

大家知道，FTP服务的默认端口是21，WWW服务的端口是80，邮件服务的端口是25、100……从安全角度来考虑，这些端口都是最容易引起攻击的，所以建议将其更改。设置方法如下：在“FTP 站点”标签页中，将“TCP 端口”文本框中的数字“21”删除后，输入一个系统中没有使用的端口号（如“98”）。



设置端口

在为FTP服务器指定了一个非21的端口号（如98）后，再使用客户端访问时，就不能仅靠输入IP地址来访问FTP服务器了，而应同时指定端口号，如“ftp://192.168.1.13:98”。

10.2.4 设置客户端连接数

为了保证FTP服务器的稳定性，就要对客户端的连接数量进行严格控制。一般来说，可以将1Mbps带宽的FTP服务器设置为允许100个连接，连接超时一般可以设置为2分钟（120秒），这样超过2分钟还没有成功连接的客户端就会被断开，以释放连接。



设置连接限制

10.2.5 访问FTP服务器

在经过上述设置后，客户端用户就可以访问FTP服务器了。因为我们已经为当前FTP服务器设置了访问IP地址为“192.168.1.13”，并且将访问端口设置为“98”，所以在IE、CuteFTP和FTP命令行方式的登录中，应分别进行如下设置才能访问FTP服务器。

1. 使用IE浏览器登录FTP服务器

在客户端电脑中启动IE浏览器后，在地址栏中输入“ftp://192.168.1.13:98”并按Enter快捷键，随后就可以访问FTP服务器了。



访问FTP服务器

从上图中可以看出，FTP服务器中已经建立了“上传”和“下载”两个目录。显然，此时客

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十章 服务器搭建、配置与管理

户端用户可以很方便地进行上传或下载操作了。

2. 使用CuteFTP登录FTP服务器

CuteFTP 是目前使用最为广泛的一种 FTP 客户端软件，它可以稳定上传或下载 FTP 服务器的数据（支持断点续传）。下面来看看怎样使用它来登录上述建立的 FTP 服务器。

在安装好并运行 CuteFTP 后，将会弹出一个对话框，要求设置 FTP 服务器的登录信息。首先需要为 FTP 设置一个名称，如“狂风 FTP”（需根据实际情况进行设置），如下图所示。然后，单击“下一步”按钮继续。



设置名称

接着根据提示设置 FTP 服务器的访问 IP 地址，然后单击“下一步”按钮继续。在输入用户名和密码的界面中，勾选“匿名登录”和“掩饰密码”两个选项后，单击“下一步”按钮继续。



勾选“匿名登录”、“掩饰密码”

接着，指定访问 FTP 服务器时同步显示的本地目录，建议将该目录设置为专用于上传或下载

数据的目录，然后单击“下一步”按钮继续。在下一步界面中，单击“完成”按钮结束设置。



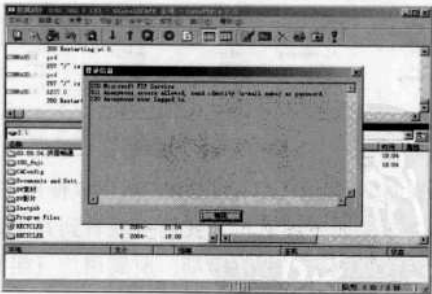
完成设置

进入 CuteFTP 主界面后，按 F4 快捷键打开“站点管理器”对话框，将右下侧的“FTP 站点连接端口”设置为“98”后，单击“连接”按钮。



开始连接

稍后，CuteFTP 将会自动登录到 FTP 服务器。



登录服务器

3. 使用FTP命令行方式访问FTP服务器

除了可以使用上述方法登录 FTP 服务器之外，还可以使用 FTP 命令来访问 FTP 站点。下面以 Windows XP 下的 DOS 命令界面为例，讲解一下



使用 FTP 命令登录 IP 地址为 192.168.127.128 的 FTP 服务器的方法。

在 DOS 命令提示符下，输入“ftp 192.168.127.128”并按 Enter 快捷键确认，然后系统会提示输入用户账号，接着又会提示输入相应的密码。如果输入的账号和密码正确，则会出现“ftp>”的提示符。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\tphl>ftp 192.168.127.128
Connected to 192.168.127.128.
220 Serv-U FTP Server v4.0 for WinSock ready...
User (192.168.127.128:(none)): FTPUser
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp>
```

输入账号密码



由于 FTP 命令是从 UNIX “流传”下来的，所以该命令的使用习惯和 UNIX/Linux 非常相似，例如，登录 FTP 服务器时并不显示输入的密码。

接下来，在“ftp>”提示符下输入适当的命令，即可对该 FTP 服务器上的文件(或目录)进行管理。要了解 FTP 支持哪些命令，可以在“ftp>”提示符下输入“?”并按 Enter 快捷键，即可看到如下图所示的信息。

```
ftp> ?
Commands may be abbreviated.  Commands are:

!                delete      literal          prompt          send
!                debug       ls               put              status
!                dir          delete          quit            trace
!                disconnect  mkdir           quote           type
!                get          mget            rcv             user
!                glob        mls             rename          verbose
!                hash        mput            rmdir
!                lcd          mput            rmdir
```

了解FTP支持的命令

例如，要显示主目录下的内容，可以使用“dir”命令，结果如下图所示，我们可以看到其下每个目录的权限属性、创建日期、所属用户(组)和文件(或目录)名等信息。

```
ftp> dir
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
drwxr-xr-x  1 user  group    8 May 3 06:58 .
drwxr-xr-x  1 user  group    8 May 3 06:58 ..
drwxr-xr-x  1 user  group    8 May 2 12:00 Software
drwxr-xr-x  1 user  group    8 Apr 26 16:28 网络工具
226 Transfer complete.
ftp: 247 bytes received in 0.015seconds 24.70kbytes/sec.
```

显示主目录下的内容

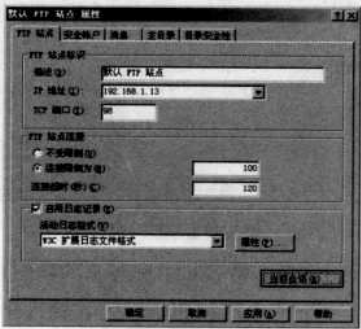
然后，可以用“cd”命令切换到合适的目录下，再用“get”(或“send”)命令来下载(或上传)指定的文件，最后可以用“quit”命令退出。虽然不太直观，但是使用起来还是很方便。

10.2.6 FTP服务器的管理

作为网管，对 FTP 服务器的了解绝不能仅仅只是会架设这么简单，一位合格的网管至少应该对 FTP 服务器的管理有一定的了解。

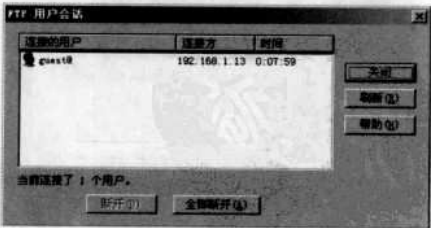
1. 会话管理

会话管理主要用于查看当前有哪些用户登录到 FTP 服务器。要打开会话管理对话框，需要单击 FTP 站点属性对话框的“FTP 站点”标签页中的“当前会话”按钮。



当前会话

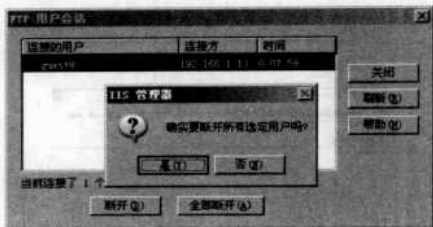
在稍后打开的“FTP 用户会话”对话框中，可以看到当前登录 FTP 服务器的用户名、来源 IP 和登录时间等信息。



显示用户名、来源IP等信息

此时，如果看谁“不顺眼”，只需选中他，然后单击“断开”按钮，并且在弹出的对话框中单击“是”按钮，即可把他“踢”出 FTP 服务器的登录用户列表。

第十章 服务器搭建、配置与管理



断开连接

2. FTP账号管理

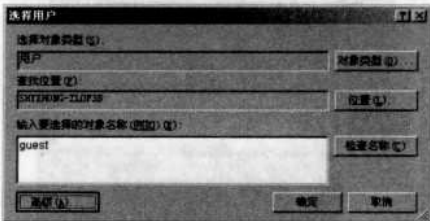
在 FTP 站点属性对话框中单击切换到“安全账号”标签页，在这里可以指定登录到 FTP 服务器的匿名客户请求的 Windows 账号，以此来控制使用服务器的用户。

单击勾选“允许匿名连接”选框，即可允许 FTP 客户端用户以匿名账号和密码（电子邮件地址）登录到 FTP 服务器。



允许匿名登录

此处可以规定所有匿名用户所使用的用户名，IIS 默认以“USER-UserName”作为匿名用户的“映射”账号（此处的 UserName 是指当前的登录用户账号）。如果希望更换一个新的账号，可以单击右侧的“浏览”按钮，在弹出的“选择用户”对话框中，可以在“输入要选择的对象名称”文本框中直接输入所需的用户名，也可以单击其上的“高级”按钮。



输入要选择的对象名称

随后，单击“立即查找”按钮，即可显示本地机上的所有用户，选择其中的一个用户（这里选择“Administrator”），再单击“确定”按钮即可。



选择一个用户

选定用户后，如果勾选了“只允许匿名连接”项，那么客户端用户就不能使用别的账号和密码登录 FTP 服务器了，而只能以匿名账号和密码（电子邮件地址）登录。这样就可以防止某些恶意用户窃取高权限账号进行登录，以确保一定的安全性。

3. 定制应答消息

当登录 FTP 服务器时，细心的读者朋友往往会发现有些服务器会显示欢迎信息，比如，显示来客的当前 IP 是多少，目前本服务器共有多少人在使用、下载的注意事项等，这些让人看起来感觉很专业。其实在 IIS 中同样也可以很轻松地设置这些显示信息。

单击切换到“消息”标签页，大家可以看到有“标题”、“欢迎”、“退出”和“最大连接数”等设置项，我们可以在这些文本框中创建自己的消息。当用户连接到 FTP 服务器时，将向用户显示这些消息。

欢迎：当客户端首次连接到 FTP 服务器时，将向其显示的 FTP 服务器消息。消息默认为空。

退出：当客户端断开与 FTP 服务器的连接时，将向其显示的 FTP 服务器消息。消息默认为空。

最大连接数：FTP 服务器所支持的客户端连接数已达到最大，而客户端仍试图连接 FTP 服务器时，将向其显示的 FTP 服务器消息。



当各个部分的消息输入完毕后，即可单击“确定”按钮完成本次设置。

当使用 CuteFTP 这样的 FTP 客户端程序访问该 FTP 服务器时，就能看到相应的应答消息了。

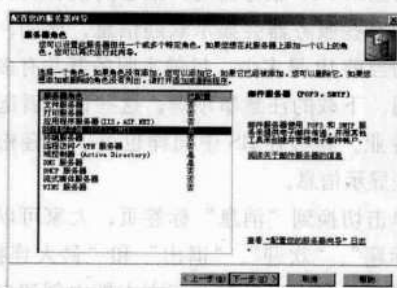
10.3 用IIS6.0架设邮件服务器

在 Windows Server 2003 中内置的 IIS 6.0 组件，已经一改昔日只能发不能收的那种令人恼火的设计，如今也可以“收发”自如了！下面就来通过 IIS6.0 完成一个拥有 POP3 和 SMTP 服务的小型邮件服务器架设吧！

10.3.1 安装组件

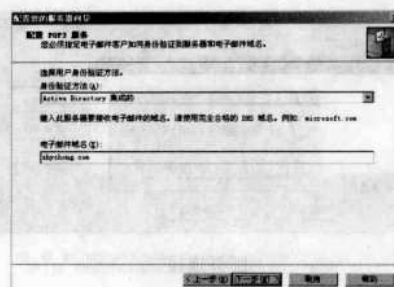
因为在 Windows Server 2003 中，默认状态下是没有安装 POP3 和 SMTP 服务组件的，所以首先要手工添加这两个组件才行。

依次点击“开始→管理工具→管理您的服务器”菜单项，在弹出的界面中单击“添加/删除角色”超级链接。在接着的“服务器角色”对话框中，选中“邮件服务器 (POP3,SMTP)”项后，单击“下一步”按钮继续。



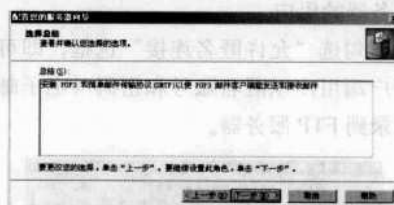
选中“邮件服务器 (POP3,SMTP)”项

接下来在“配置 POP3 服务”对话框中，在“选择用户身份验证方法”下拉列表中选择用户身份验证的方式。其中默认会有 Windows 账户身份验证和加密码文件身份验证两种方式。如果该计算机升级为域控制器，就会有 Active Directory 集成的身份验证和加密码验证两种方式。接着在“电子邮件域名”中输入电子邮件的域名，如 shyzhong.com。



输入电子邮件的域名

在“选择总结”对话框出现时，将 Windows Server 2003 安装光盘放入光驱，在单击“下一步”按钮后，组件将开始安装。



开始安装组件

稍后系统将自动从 Windows Server 2003 安装光盘中提取文件至系统中，从而完成 POP3 服务器与 SMTP 服务器组件的安装。当出现“此服务器现在是邮件服务器”界面时，表示邮件服务器已经安装成功。

接着，在“控制面板→添加/删除程序→添加/删除 Windows 组件”中，选中“电子邮件服务”和“POP3 服务 Web 管理”两项安装，具体的使用方法将会在下面讲解。



选中“POP3服务Web管理”

第十章 服务器搭建、配置与管理

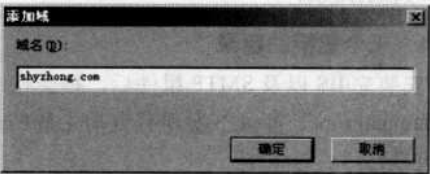
10.3.2 配置POP3服务器

因为POP3服务器和SMTP服务器需要分别进行设置，所以这里先来对POP3服务器进行配置。首先需要创建一个邮件域，方法是：点击“开始→程序→管理工具→POP3服务”菜单项，在弹出的“POP3服务控制台”窗口中，选中左侧的“POP3服务”下的服务器名（这里为SHYZHONG-ZLOF3B）后，点击右侧的“新城”项。



点击“新城”

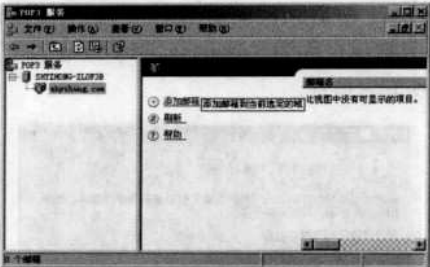
接着将弹出“添加域”对话框，首先在“域名”栏中输入邮件服务器的域名，也就是邮件地址“@”后面的部分（如“shyzhong.com”），接着点击“确定”按钮。



输入邮件服务器的域名

为了确保架设的POP3服务器可以正常在Internet上运行，“shyzhong.com”之类的域名应为Internet上注册过的域名（POP3服务支持顶级以及三级域名，例如shyzhong.com和js.shyzhong.com都是受支持的），并且该域名还要在DNS服务器中设置了MX邮件交换记录，才能正确解析到Windows Server 2003邮件服务器的IP地址上。这个过程的操作方法，请查阅申请Internet域名时服务商给出的资料。

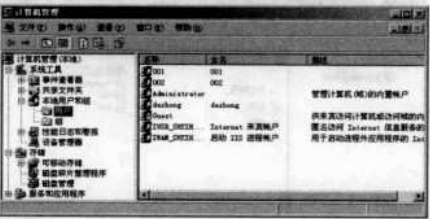
在域添加完毕后，就可以进行用户邮箱的创建了。选中刚刚创建的“shyzhong.com”域，在其右侧点击“添加邮箱”项。



点击“添加邮箱”

在弹出的“添加邮箱”对话框中的“邮箱名”栏中输入邮箱账户名（如dazhong），然后为该账户设置密码后，点击“确定”按钮完成邮箱的创建。

注意对话框中的“为此邮箱创建相关联的用户”项，这是指可以为当前创建的邮箱账户在系统中同步创建一个同名用户。这一点在“计算机管理”窗口的“本地用户和组”下的“用户”列表中就可以看出来了。



同步创建一个同名用户

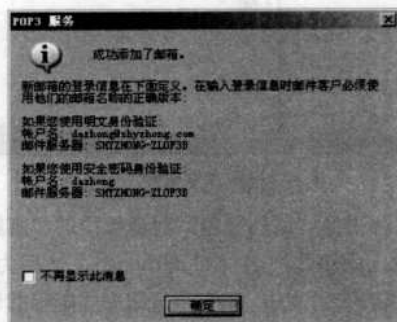
从列表中可以看到系统中已经创建了一个名为“dazhong”的用户了，这个用户名和刚创建的邮箱用户名是相同的。如果查看该账户的属性，则可以在“隶属于”选项卡设置界面中发现该账户隶属于“POP3 Users”组。



查看账户的属性

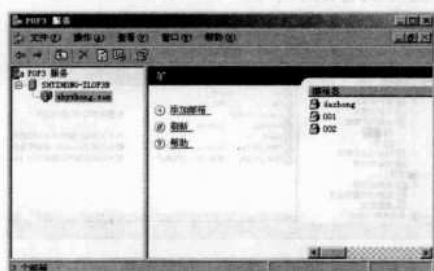


接着，在弹出的提示框中，可以看到刚创建的电子邮箱全称为“dazhong@shyzhong.com”以及一些其它信息。



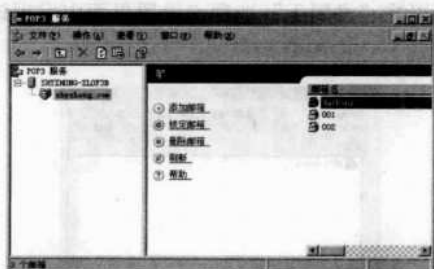
电子邮箱相关信息

显然，已经成功添加了一个邮箱。在返回到POP3 服务窗口后，在选中“shyzhong.com”域后，可以在右侧看到创建的邮箱名列表。



邮箱列表

当选中的一个邮箱后，在窗口的中间部分将会出现“锁定邮箱”、“删除邮箱”等几个选项。



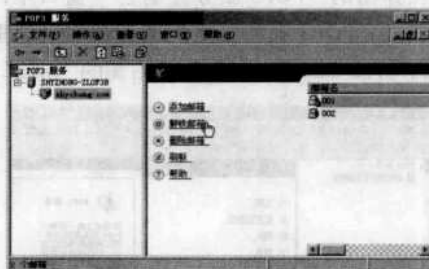
锁定邮箱、删除邮箱

在某些邮箱用户不再需要时，可以点击“删除邮箱”项将其删除掉。为了安全考虑，在弹出的“删除邮箱”对话框中勾选“同时也删除与此邮箱相关联的用户账户”项。点击“是”按钮后，

210

就可以将当前选中的邮箱及系统中相应的账户删除了。对于一些暂时不方便删除，却又暂时不打算使用的邮箱，则可以在选中邮箱的同时，点击“锁定邮箱”项来完成当前邮箱的锁定操作。

在锁定邮箱后，在需要启用该邮箱时，只需在选中该邮箱的同时，点击“解锁邮箱”项即可。



解锁邮箱

10.3.3 配置SMTP服务器

在完成POP3 服务器的配置后，先不要急着对SMTP 服务器进行配置，建议大家先了解一些SMTP 的基本知识。这样不仅有助于了解以后配置SMTP 服务器时的一些选项，还对使用SMTP 服务时极有帮助。

1. 七个重要的目录

安装完IIS 以及SMTP 组件后，将会在“X:\Inetpub\mailroot”目录下发现有自动生成的七个工作目录。



七个工作目录

这七个文件夹的名字及各自的作用是：

Badmail：死信目录，该文件夹用来存放错误邮件。所谓错误邮件，是因为诸如收信人邮件地

第十章 服务器搭建、配置与管理

址错误、收信人的邮件服务器出错或网络故障而导致邮件无法到达，SMTP 虚拟服务器会自动产生一份错误报告，与原邮件一起退还给发信人。如果退回邮件时也发生错误，则该数据就会保存在 Badmail 文件夹里。

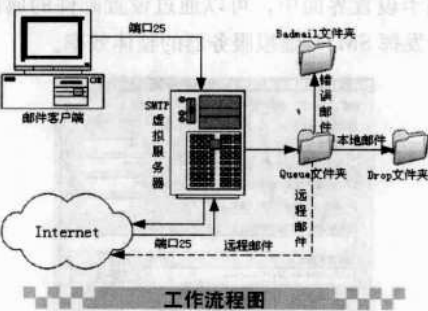
Drop：存放本地邮件的地方，邮件文件的扩展名是 elm。

Pickup：当使用邮件客户端程序写好邮件，并单击“发送”按钮，该邮件即可暂存于这个 Pickup 文件夹。系统会定期检查该文件夹，一旦发现邮件，就会进行及时处理：或是将邮件转到 Drop 文件夹，或者将该邮件转发到远程的邮件服务器。

Queue：存放正在处理的邮件的临时文件夹。
Mailbox、Route 和 SortTemp：这三个文件夹是 SMTP 虚拟服务器在整理、分类时所使用的的工作目录，工作结束后，系统将会自动清空这些文件夹。

2. SMTP的工作原理

为了让大家了解 SMTP 虚拟服务器的工作原理，下面对其工作流程作一简单介绍。当系统发现 Pickup 目录里有邮件存在，或者有邮件从 25 端口进入该目录，服务器会将该邮件自动转移到 Queue 目录。如果是本地邮件，则会将其转入 Drop 目录。如果是远程邮件，则服务器将会启用远程传递程序进行处理。整个工作流程如下图所示。



本地邮件处理：前面已经说过，如果 SMTP 虚拟服务器发现邮件的目的地是本地收件人，则

会把该邮件从 Queue 目录转移到 Drop 目录，它的任务就算完成了。我们可以在随后的章节里学习如何指定 Drop 文件夹的路径。

远程邮件处理：SMTP 虚拟服务器会尝试与接收邮件服务器进行连接。如果该接收服务器尚未准备好，则邮件会继续保留在 Queue 目录下，经过指定的时间间隔后，服务器会尝试再次连接，如果连接成功，就会将邮件发出。如果经过指定的次数还是未能连接成功，则会认为该邮件是错误邮件，该邮件连同错误报告将会一起被转入 Badmail 目录。

3. 启动与停止服务

依次点击“开始→程序→管理工具→Internet 信息服务 (IIS) 管理器”菜单项，在弹出的“Internet 信息服务 (IIS) 管理器”窗口中右键点击“默认 SMTP 虚拟服务器”选项，在弹出的菜单中可以看出安装好 IIS 以及 SMTP 组件后，SMTP 服务就已经自动启动了。

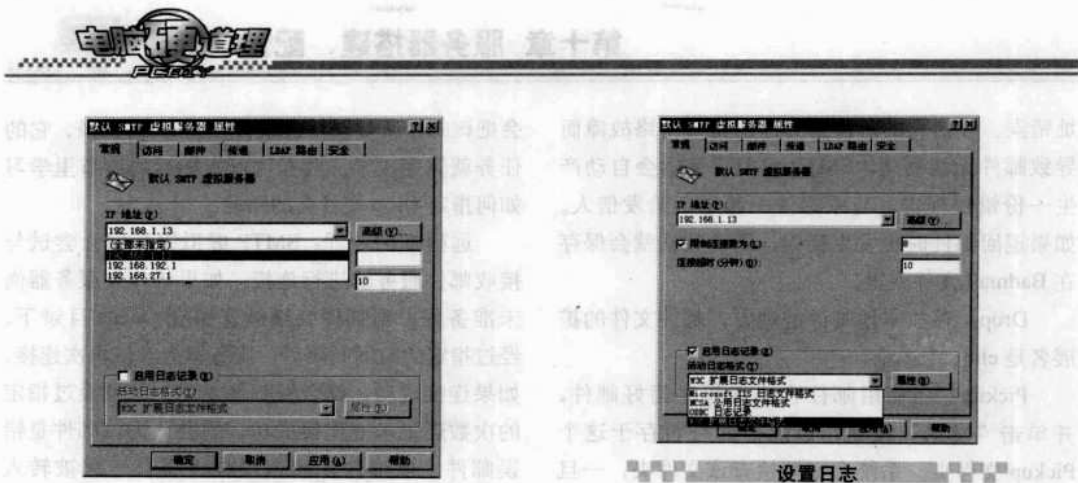


点击“默认 SMTP 虚拟服务器”

如果需要停止服务，只需点击快捷菜单上的“停止”项就可以了。

4. 指定 IP 地址

右键点击“默认 SMTP 虚拟服务器”选项，在弹出的菜单中选择“属性”项，打开“默认 SMTP 虚拟服务器 属性”窗口的“常规”选项卡下，点击“IP 地址”项右侧的下向箭头，在弹出的 IP 地址列表中选择用于 SMTP 服务的一个后，点击下方的“应用”按钮即可。



指定IP地址

5. 设置连接数

在“常规”选项卡设置界面中，为了确保SMTP虚拟服务器的性能，可以勾选“限制连接数”复选框，并指定具体连接数（默认为10，这里指定为8），还可以指定连接超时的分钟数（默认为10分钟）。




设置连接数

6. 设置日志

我们还可以使用日志记录跟踪服务器通过网络从SMTP客户端接收的命令。要想使用日志功能，必须勾选“常规”选项卡设置界面中的“启用日志记录”复选框，这里共有4种日志记录格式，分别是“Microsoft IIS 日志文件格式”、“NCSA 公用日志文件格式”、“ODBC 日志记录”和“W3C 扩展日志文件格式”，默认为“W3C 扩展日志文件格式”。

单击右侧的“属性”按钮，还可以对日志文件的属性进行设置。

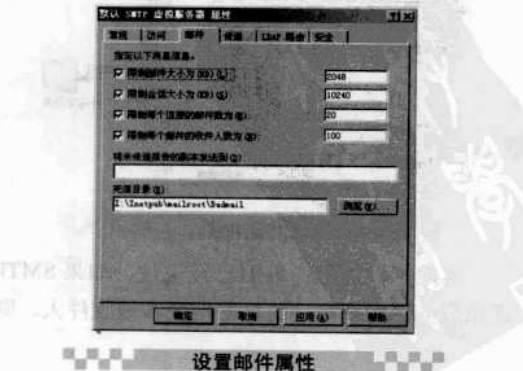
在弹出的“日志记录属性”对话框的“常规”选项卡设置界面中，可以指定W3C扩展日志的记录计划、文件大小。还可以自定义保存路径，默认保存在“X:\WINDOWS\System32\LogFiles\SmtpSvc1”目录中。

**注意**

文件名随日志记录格式的不同而不同，例如，W3C扩展日志的文件名为exymmdd.log（此处的ymmdd由具体的年、月、日所替代），而NCSA公用日志的文件名为ncyyddmm.log。

7. 邮件限制

在SMTP虚拟服务器“属性”窗口中的“邮件”选项卡设置界面中，可以通过设置邮件的属性来充分发挥SMTP虚拟服务器的整体效率。



设置邮件属性

第十章 服务器搭建、配置与管理

例如，邮件的大小、一次会话所能容纳的所有邮件的总量大小、每次连接的最多处理邮件数量、一信多投的最多收件人数等。

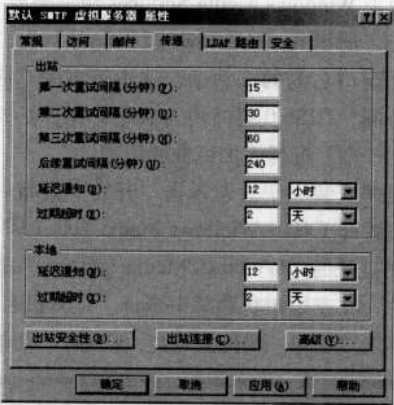
注意

“将未传递报告的副本发送到”功能是指：如果由于某种原因未能发送邮件，则系统会将该邮件退还给发件人，同时还会产生一个未传递报告（NDR），我们可以把未传递报告（NDR）的副本发送到一个指定的 SMTP 邮箱。在“将未传递报告的副本发送到”文本框里输入该 SMTP 邮箱名即可。

此处还可以指定死信目录的地址，默认是“X:\Inetpub\mailroot\Badmail”，点击“浏览”按钮话可以进行自定义选择。

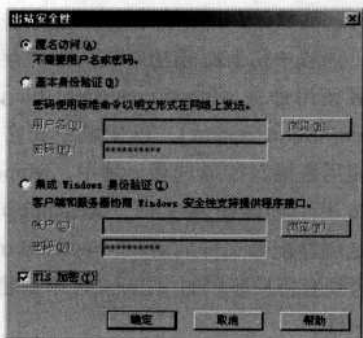
8. 设置传递项

在 SMTP 虚拟服务器“属性”窗口中的“传递”选项卡设置界面中，可以设置邮件发送出现错误时的重试时间等设置。



设置发送出错的重试时间

若要启用远程传递的传输层加密机制（Transport Layer Security，简称为 TLS），让 SMTP 虚拟服务器将所有输出的邮件加密，则可以单击对话框中的“出站安全性”按钮，然后在弹出的对话框中勾选“TLS 加密”复选框项即可。



设置加密传输

9. 邮箱的大小设置

用户对信箱最关心的事情莫过于其容量的大小了。Windows Server 2003 的 POP3 邮件服务器可以通过启用磁盘配额来限制一个账户的磁盘空间，以实现对应的邮箱大小的设置。这样既防止了用户无限制地使用磁盘空间，又保护了用户邮件的安全。

注意

根邮件目录必须创建在 NTFS 格式的硬盘分区中，否则系统将无法实现磁盘配额。

如果邮件服务器采用活动目录集成的身份验证或本地 Windows 账户身份验证，那么在为用户创建邮箱时，默认将创建一个配额文件，并启用相应的磁盘配额。因此，如果用户信箱采用默认的磁盘限额设置，就不必再为每个用户进行单独的设置。

（1）启用磁盘配额功能

由于该磁盘配额功能默认适用于全部电子信箱，因此应当充分考虑到磁盘的总容量、用户总数量等因素，以合理地设置磁盘限额功能。

（2）为个别用户单独设置磁盘限额

对于一些对信箱容量有特殊要求的用户，可以单独为其设置磁盘配额。为了简化操作，可以先创建一个邮箱和用户账户作为模板，并为其指定磁盘配额。



然后，从域账户的邮件存储目录中将该配额文件拷贝到域中所有邮箱相对应的邮件存储目录中，或者使用命令 `winpop createquotafile username@domain[/user:username]`，以使域中其它的指定账户将使用该磁盘配额选项。其中，`winpop createquotafile` 用于创建配额文件，`username@domain` 用于指定创建配额文件的用户，`/user:username` 选项将参考现有用户账户的 配额文件来创建一个新的配额文件。

10.3.4 测试SMTP服务

在完成上述设置后，就可以使用邮件客户端软件连接邮件服务器进行邮件收发工作了。以 Foxmail 为例，在新建一个账户后，要注意在“账户属性”窗口中的“邮件服务器”项里设置服务器的域名为“shyzhong.com”。

这样今后不管发送多大的邮件，都是“闪电速度”，因为根本不需要通过因特网发送到 ISP 指定的 SMTP 服务器，而只需要发送到本机即可，剩下的事情就交给 SMTP 虚拟服务器去处理吧，它会自动帮助我们吧邮件转发到指定的目标，再也不需要忍受 ISP 提供的 SMTP 服务器那蜗牛般的速度了！



注意

Windows Server 2003 还支持对邮件服务器的远程 Web 管理。在远端客户机中，运行 IE 浏览器，在地址栏中输入“https:// 服务器 IP 地址:8098”，将会弹出连接对话框，输入管理员用户名和密码，点击“确定”按钮，即可登录 Web 管理界面。

10.4 用IIS6.0搭建流媒体服务器

在局域网中，同步收看各种教学、业务视频现在是很时尚的应用。如果你也想架设这样的一台既可以进行网络广播，又可以进行视频点播的流媒体服务器，供局域网们进行实时视频交流。那么，就请跟随本节一起来学习在 Windows

Server 2003 中，架设流媒体服务器以及对其进行远程管理的方法。



注意

流媒体是实况或预录制的音频和视频内容，通过网络或 Internet 传递到客户端计算机。与下载的文件不同，当流媒体内容传输结束之后，不会在用户硬盘中保存任何数据。

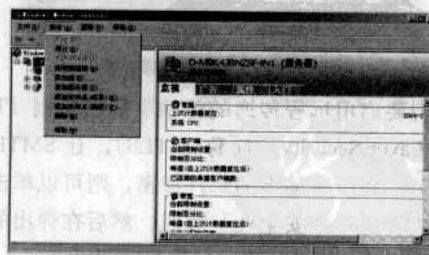
10.4.1 架设流媒体服务器

因为 Windows Server 2003 中内置了流媒体服务器组件，所以架设既支持网络广播又可进行视频点播的 Windows Media 流媒体服务器是一件很容易的事情。

依次点击“开始→设置→控制面板→添加或删除程序”，在弹出的窗口中选择“添加/删除 Windows 组件”，在随即弹出的“Windows 组件向导”窗口中点击选中“Windows Media Services”项。

因为 Windows Media Services 组件需要 IIS6.0 的支持，所以在“Windows 组件向导”窗口中还应拖动窗口右侧的滚动条，选中下方的“应用程序服务器”（IIS6.0 组件内含其中）组件后，再单击“下一步”进行添加组件的添加。

组件安装完毕后，单击“开始→设置→控制面板→管理工具→ Windows Media Services”菜单项。在打开的“Windows Media Services”管理器窗口中，在左边树状菜单中选择“计算机名”后，依次单击“操作→添加发布点（向导）”菜单项。



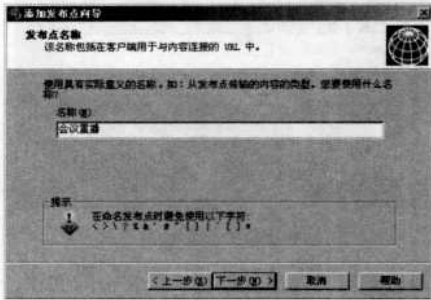
添加发布点

稍后将进入“添加发布点”向导页面，点击

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

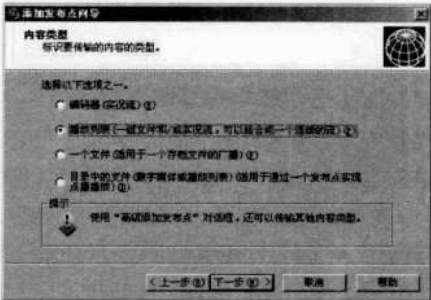
第十章 服务器搭建、配置与管理

“下一步”按钮继续。下一步中需要设置一个“发布点名称”，根据提示，可以得知名称的设置要求。



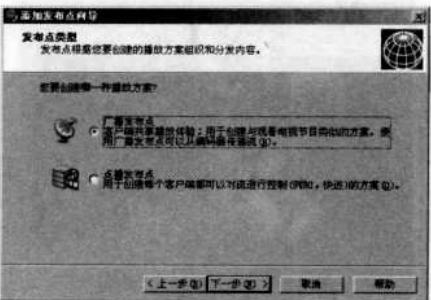
输入发布点名称

在接下来的窗口中，选择将要发布的文件类型，如果是进行实况直播，可以选择“编码器（实况流）”。由于已经有了制作好的电影文件，所以这里选择第二项“播放列表”。



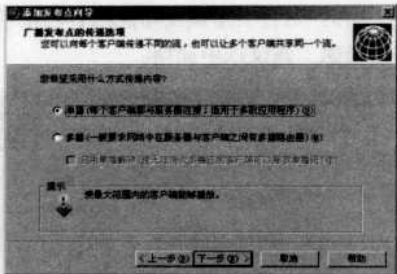
选择第二项“播放列表”

接着选择将要创建的播放方案，由于即将要创建的是广播站，因此只能选择“广播发布点”。



选择“广播发布点”

再在接下来的传递方式中选择“单播”。



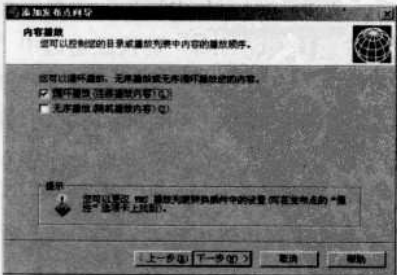
选择“单播”

在下一步的传输内容窗口中选择“新建播放列表”（如果以前制作过播放列表，可以直接选择“现有播放列表”）。在新建播放列表窗口中，点击“添加媒体”按钮。接着在弹出的“添加媒体元素”对话框中点击“浏览”按钮，找到媒体文件所在的目录并选择相应文件进行媒体文件的添加（包括所有支持的流媒体文件、远程发布点、来自编码器的流媒体、播放列表、目录中的文件等等）。



添加媒体元素

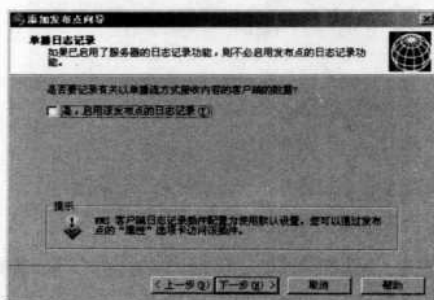
完成新建列表的编辑后，点击“下一步”将播放列表文件保存。接着根据实际情况选择是“循环播放”还是“无序播放”。建议选择“循环播放”，因为这样相对控制起来容易些。



选择“循环播放”



在下面的“是否启用该发布点的日志记录”中，基于安全考虑，建议选中此项。



选择启用该发布点的日志记录

在下面的“发布点摘要”中，选择默认状态并点击“下一步”按钮继续。最后单击“完成”即可完成 Windows Media 网络广播服务器的架设。

如果在选择了“创建公告文件 (.asx) 或网页 (.htm)”项，那么还会启动一个单播公告向导，这里可以单击“是”按钮创建一个带有嵌入的播放机和指向该内容的链接的网页，从而实现直接生成 html 文件以便发布到互联网上。在下一步的“访问该内容”对话框中，可以直接点击“下一步”按钮选择默认状态继续。



“访问该内容”对话框

在下一步的“保存公告选项”中将需要指定保存的文件路径和文件名。建议点击选中“创建一个带有嵌入的播放机和指向该内容的链接的网页”项，以便客户端可以使用 http 方式访问网页。

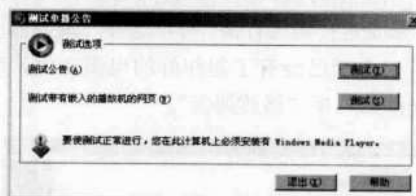
下一步中需要设置在客户端使用 Windows Media Player 播放流媒体文件时，显示的公告数据。这里可以在选中需修改项后，在点击出现编辑状态后进行修改。



更改显示公告数据

最后单击“完成”按钮结束文件的创建。

由于选中了“完成此向导后测试文件”项，所以稍后弹出“测试单播公告”界面。



测试单播公告

从图中可以看到有两个测试选项，一个是“测试公告”；另一个是“测试带有嵌入的播放机的网页”；分别点击两个项右侧的“测试”按钮后，可以看出调用 Windows Media Player 测试服务器是否架设成功。第一个“测试”按钮按下后，将调用 Windows Media Player 播放器进行播放；第二个“测试”按钮按下后将调用 IE 窗口对创建的内嵌播放器的网页文件进行测试。



进行测试

从上图中可以看出测试是成功的，因为内嵌播放器的网页中正在使用内嵌的播放器进行流媒体服务器中的媒体文件播放。

经过上述设置后，网络中的客户端用户就

第十章 服务器搭建、配置与管理

可以在 IE 浏览器的地址栏中或 Windows Media Player 播放器的“文件→打开 URL”栏中输入：
mms:// 服务器 IP 地址 / 发布点名称，
这样的格式对架设的流媒体服务器进行网络广播式的媒体文件欣赏了。

10.4.2 Web接口管理

令人兴奋的是，在 Windows Server 2003 中，流媒体服务器可以通过 Web 接口来管理了。实现方法如下：
依次点击“开始→设置→控制面板→添加或删除程序”，在弹出的窗口中点击“添加或删除 Windows 组件”，在弹出的“Windows 组件向导”窗口中点击勾选“Windows Media Services”选项，并双击打开该选项的详细设置窗口，点击勾选“用于 Web 的 Windows Media Services 管理器”项。从随之弹出的“Windows Media Services 安装警告”提示框中，可以看到当前选中的组件需要 IIS 6.0 的支持。此时点击“确定”按钮（IIS6.0 组件将会随之被自动选中）。



安装IIS组件

在上述组件安装完毕后，就可以在远程计算机的 IE 浏览器地址栏中输入如下网址，使用 Web 接口管理流媒体服务器了：
http:// 流媒体服务器 IP 地址 :8080/，
如：http://192.100.100.16:8080/default.asp。



注意

根据服务器的安全设置不同，有可能需要输入管理员用户名和密码才能出现上述页面。

输入网址并按回车键后，就可以看到 Windows Media Services 的 Web 接口管理页面了。
以远程开启或关闭发布点为例，操作过程如下：
点击上图中“管理本地 Windows Media 服务器”链接，进入流媒体服务器的管理页面。在左侧部分可以看到“发布点”列表。



“发布点”列表

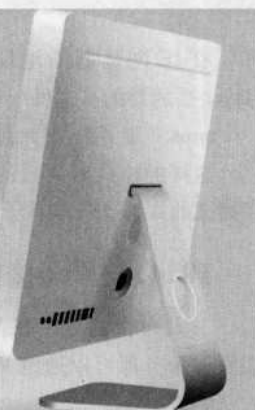
选中左侧“发布点”列表中的 Sample Broadcast 项，在页面右侧部分随之切换到相应的设置面板时，点击切换到“源”选项卡设置页面。



“源”选项卡设置页面

看到右侧部分下方的一排按钮了吗？点击相应的按钮即可执行相应的操作了，如点击“停止”按钮就可以即时关闭该发布的“启动”状态了。
要提醒大家注意的是，为了安全考虑（防止其它用户管理 Windows Media Services），在退出 Web 接口管理页面时，最好输入类似以下网址来注销本次管理。
http://192.100.100.16:8080/WMSLogOff.asp，
回车后弹出的管理页面中，只需点击“关闭”按钮即可。

第十一章 网络升级与优化实战



经过不断的技术革新和软硬件的更新换代，在几年前组建的局域网已经远远落后于目前的网络配置。为了局域网能好地服务于用户的工作，建议升级改造原有的局域网，并对网络性能进行必要的优化。出于保护原有投资的考虑，在尽量保留原有设备的前提下提升网络性能是本章讨论的焦点问题。

11.1 硬件设备升级

网络带宽的提升有赖于相应的硬件设备的支持，下面将从局域网中必不可少的网卡、网线、HUB（集线器）、交换机和服务器等方面入手，谈一谈跟提升网络带宽有关的硬件设备的升级。

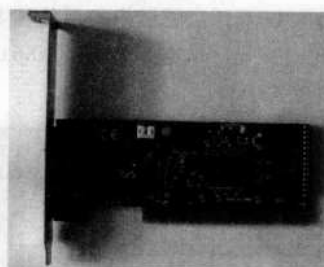
11.1.1 升级分析

首先针对目前大多数局域网的现状进行一下简单分析，然后提出大概的升级意见。

1. 网卡

随着 PCI 接口网卡的迅速普及，现在无论在服务器中还是工作站中已很难觅到 ISA 接口网卡的踪迹了。因为无论是从功能上还是从数据传输的速度上来比较，PCI 网卡都大大优于 ISA 网卡。因此，如果具备更换成 PCI 网卡的条件，就应该坚决淘汰掉 ISA 网卡。

目前市场上的主流网卡是 PCI 接口的 10M/100M 自适应网卡，价格相对而言也是比较便宜的。将服务器或工作站的网卡升级成 10M/100M 自适应 PCI 网卡所带来的局域网整体性能的提升将是非常显著的，况且这也是网络接口、网络速度的主流标准。



10M/100M自适应网卡

2. 网线

目前，超五类双绞线占据着绝大多数的市场份额。无论在性能上还是在质量上，超五类双绞线都明显优于过去使用的同轴电缆。如果很不幸，用户现在管理的网络使用的就是同轴电缆，那么在网卡升级至 10M/100M 自适应 PCI 网卡后，网线的升级必不可少。

正所谓“好马配好鞍”，网络瓶颈的产生往往就是由于网络内硬件设备配合使用不合理而引起的。同时需要提醒的是，对网线的升级不仅仅只是线路的改变，更重要的在于网络性能、传输速度和管理维护的需要。

第十一章 网络升级与优化实战



超五类双绞线及水晶头

3. HUB

对于HUB的升级，10M/100M自适应的HUB似乎成了标准的升级配置，只有这样才能跟已经升级的网卡和网线相匹配。并且考虑到以后局域网内机器的增多，选择网络接口尽可能多的HUB很有必要（如16口、24口）。另外，升级成10M/100M自适应HUB还可以使原先的10M HUB继续发挥余热。



10M/100M自适应HUB

4. 交换机

随着技术的进步和价格的降低，交换机已经迅速普及到现在的局域网中。如果将局域网升级成单纯的交换网络，或者在原先共享网络的基础上通过添加一台或几台交换机升级成共享、交换混合的网络，那么局域网的性能将有一个质的飞跃。



交换机实物图

5. 服务器和工作站

对服务器和工作站，可以采用更换更高主频的CPU、更换主板、增加内存容量等方法来提高机器运行速度，从而达到升级的目的。对于像无盘网络这样需要服务器提供各种服务的情况，升

级服务器的硬件配置尤为重要。因为在无盘网络中，各种应用程序和软件都是在服务器上运行的，服务器性能的好坏将直接影响着无盘工作站的工作效率。



服务器实物图

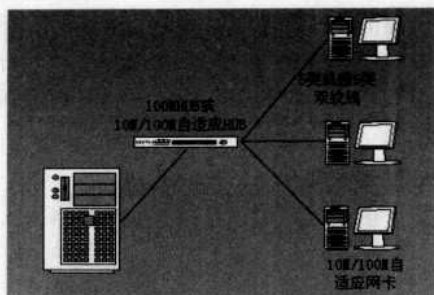
11.1.2 升级到100M共享

从10M网络升级到100M网络的最佳途径就是将局域网中所有涉及到的网络设备全部更换成100M带宽的产品，这种升级也是最简单高效的。而在实际的升级案例中，用户总是尽可能地使络中的原有设备继续发挥作用。于是这就需要兼顾最终升级目标和原有网络设备的可持续使用能力。

为了叙述的方便，以“小型10M共享网络升级到100M共享网络”和“中型10M共享网络升级到100M共享网络”作为两个升级方案。以这两个方案作为叙述载体，谈谈10M网络到100M网络的升级之路。

1. 小型10M共享网络升级到100M共享网络

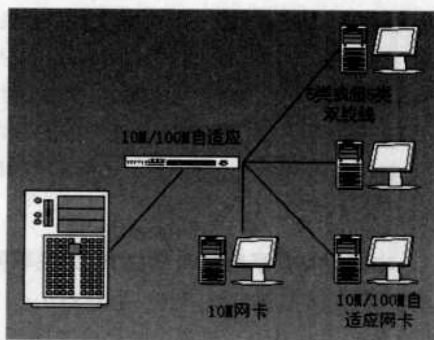
在小型10M共享网络中，一般只有1台10M的HUB作为中心节点，网络内的服务器和所有的工作站采用星型拓扑结构连接到中心节点上。升级这种形式的局域网应该考虑两种情况，一种就是网络中所有的工作站均能提供PCI总线，这时只需要将原有的10M网卡全部更换成PCI接口的100M或10M/100M自适应的网卡就行了。相应的HUB也应该换成100M或10M/100M自适应的。



小型100M共享网络

另一种情况稍微复杂一些，就是网络中有一部分计算机的性能较差，没有提供 PCI 总线，这时就应该考虑升级的整体成本了。如果更换工作站的主板使之能够提供 PCI 总线当然是最理想的升级方案，然而这会大大增加升级成本，现实意义不大。

从节约成本和稳定网络整体性能的角度出发，把能够提供 PCI 接口的计算机更换成 100M 或 10M/100M 自适应的网卡，而在较低性能的计算机中依然留用其 10M 网卡。而集线器则必须更换成 10M/100M 自适应的，在集线器和 100M 网卡之间必需使用 5 类或超 5 类双绞线，升级成 10M、100M 混合的局域网络。这样既控制了升级成本，又使局域网的整体性能有了明显的提升。



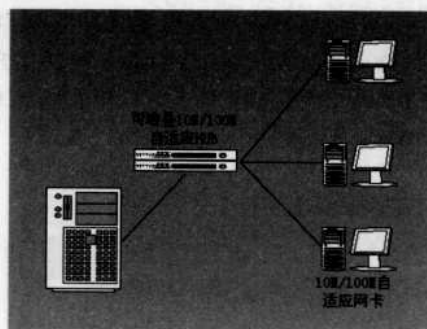
小型10M、100M混合共享网络

2. 中型10M共享网络升级到100M共享网络

在中型 10M 共享网络中，网络中拥有两台或两台以上 10M 的 HUB，其中 HUB 之间通过级联方式与中心 HUB 相连，服务器和工作站通过中心

HUB 或级联 HUB 连接在一起。相对而言，中型 10M 共享网络中的工作站数量比较多，相应的硬件配置也比较多样。针对中型 10M 共享网络的升级可按照“使用可堆叠 100M 或 10/100M 集线器”和“升级中心集线器和部分高性能计算机”两种思路进行。

第一种思路中需要在网络服务器和具有 PCI 总线的较高性能的工作站安装 100M 或 10M/100M 网卡，网线全部使用 5 类或超 5 类双绞线，而集线器则采用 100M 或 10M/100M 可堆叠式集线器，将服务器和所有工作站直接连接至可堆叠集线器上。

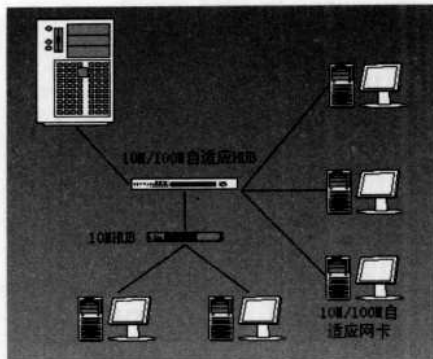


中型100M共享网络

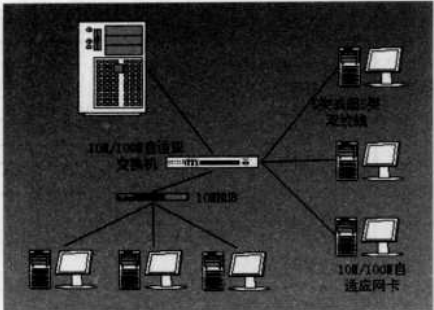
由于网线的最大数据传输距离限制在 100 米，因此如果按照第一种思路进行升级，则工作站到可堆叠式集线器之间的最大距离只有 100 米。由此可见，使用一台可堆叠式集线器连接所有的工作站受到一定的限制。如果网络的实际连接范围超过 100 米就不能通过一台可堆叠式的集线器来升级。

这时可以考虑将位于中心位置的 10M 集线器更换成一台 10M/100M 自适应的集线器，原先的 10M 集线器仍然留用。然后将硬件性能比较高（主要是指可以提供 PCI 总线）的工作站网卡更换成 100M 或 10M/100M 自适应的网卡，并直接连接到中心集线器。而对于那些性能较低的工作站则继续留用其 10M 网卡，并将这些工作站连接至 10M 的集线器。

第十一章 网络升级与优化实战



中型10M、100M共享网络



10M、100M混合交换网络

11.1.3 升级到100M交换网络

100M 交换网络所提供的交换功能可以克服共享式网络存在的网络带宽利用率低的不足，可以使每个工作站独享 100M 带宽。而且从 100M 共享升级到 100M 交换也非常方便，只要将原有的 100M 或 10M/100M 自适应集线器更换成 100M 交换机就可以完成升级。

100M 的网络比较适合大数据量的传输（如影音数据流）。然而在 100M 共享网络中，由于数据包的冲突而产生的数据频繁发送使网络信道变得非常拥挤，可想而知其网络效率非常低。升级到 100M 交换网络以后，网络中两个节点之间可以实现直接通信。

两个节点之间一旦建立通信关系，便可以使用 100Mb/s 的传输速度实现点对点的数据传输，从而有效避免了数据包的冲突，网络效率明显提高。因此，100M 交换网络为数据的有效传输提供了一个非常理想的环境。

100M 共享网络的基础上将原来的集线器更换成交换机即可完成升级，网络中原有的网卡和网线可以继续留用。如果升级以前网络中的计算机数量比较多，并且所有的计算机都是通过 100M 或 10M/100M 可堆叠式集线器进行连接时，只需要新增加一台 100M 或 10M/100M 自适应交换机，把每台集线器直接连接到交换机即可。集线器之间不必再进行堆叠，其它网络结构也可以保持不变。

11.2 操作系统升级

作为 Windows 2000 Server 的升级版本，Windows Server 2003 在继承了 Windows 2000 Server 出色的稳定性和强大的管理功能的基础上，在许多方面有了重大改进。本节内容将简要介绍从 Windows 2000 Server 升级到 Windows Server 2003 的方法步骤，希望能对读者认识和了解 Windows Server 2003 有所帮助。

11.2.1 升级准备工作

升级安装是指在基于 Windows NT 4.0（集成了 Service Pack 5 及以上版本）或 Windows 2000 Server 平台的服务器上安装 Windows Server 2003。在升级时原来服务器中的设置、用户、组、权限和许可证都会得到保留，而不用安装后重新设置。同时，升级前服务器中已经安装好的应用程序不用重新安装就可以使用。升级操作不能跨语言版本升级，比如不能从英文版的 Windows 2000 Server 升级到中文版的 Windows Server 2003。

另外，Windows Server 2003 企业版和 Windows Server 2003 数据中心版的 64 位版本只与 64 位的基于 Intel Itanium 处理器的系统兼容。它们不能被成功地安装到 32 位系统上。进行升级以前首先检查服务器的硬件配置是否达到 Windows Server 2003 的最低要求，如果原有的服务器系统硬件配置达不到要求，请根据下表列出的配置清单升级相关硬件。



Windows Server 2003各个版本对硬件的要求及支持能力

要求	标准版 Standard Edition	企业版 Enterprise Edition		数据中心版 Datacenter Edition		Web版 Web Edition
		x86	Itanium	x86	Itanium	
最小CPU速度	133MHz	133MHz	733MHz	400MHz	733MHz	133MHz
推荐CPU速度	550MHz	733MHz		733MHz		550MHz
多处理器支持	1或2	最多8个		最少8，最多32个		1或2
最小RAM要求	118MB	118MB		511MB		118MB
推荐最小RAM	256MB	256MB		1GB		256MB
最大RAM支持	4GB	32GB	64GB	64GB	118GB	2GB
驱动磁盘空间	1.5GB	1.5GB	2.0GB	1.5GB	2.0GB	1.5GB

1. 系统兼容性检查

通过检查系统的兼容性可以确认计算机的当前硬件配置与软件版本是否与 Windows Server 2003 系列产品兼容，这是升级操作之前必须要做的重要步骤之一。Windows Server 2003 的安装光盘提供了系统兼容性检查功能，具体操作如下：

STEP 1 检查兼容性。将 Windows Server 2003 安装光盘放入光驱，光盘自动运行并显示欢迎界面。单击“检查系统兼容性”按钮。



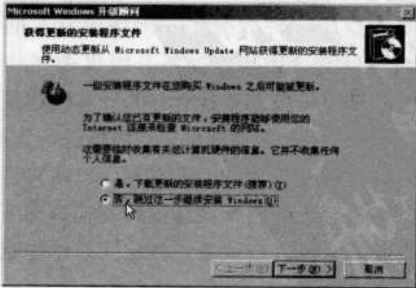
检查系统兼容性

STEP 2 选择“自动检查我的系统”。在打开的下一个界面中单击“自动检查我的系统”按钮。



自动检查系统

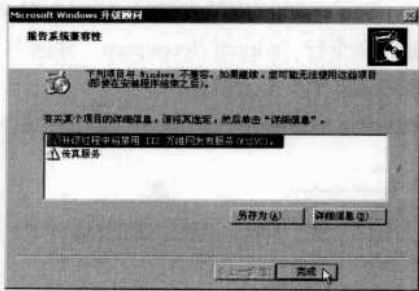
STEP 3 打开 Microsoft Windows 升级顾问。接下来检查程序会打开“Microsoft Windows 升级顾问”对话框，提示用户可以从 Microsoft 网站获得更新的安装程序文件。因为还没有进入正式的升级安装，只是想检查一下系统的兼容性，因此只需点选“否，跳过这一步继续安装 Windows”单选框，并单击“下一步”按钮。



不获取更新程序

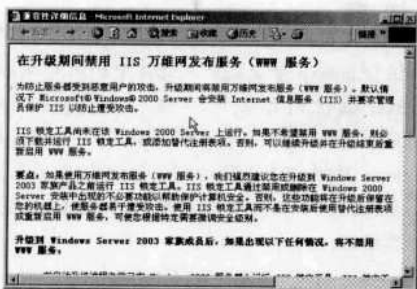
第十一章 网络升级与优化实战

STEP 4 查看不兼容的项目。等待检查程序加载系统兼容性文件并对系统进行检查，检查结束以后会报告系统兼容性结果，并在列表中列出了所有与 Windows Server 2003 不兼容的项目。单击“完成”按钮结束检查。



报告系统兼容性

STEP 5 查看详细介绍。要想解决这些兼容性问题，必须了解有关这些不兼容项目的详细资料。选中某一个项目的名称并单击“详细资料”按钮即可打开对该项目的详细介绍。



不兼容项目详细资料

注意

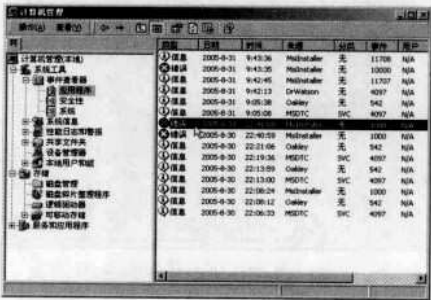
除了使用 Windows Server 2003 安装光盘进行系统兼容性检查以外，还可以利用 Microsoft 提供的在线应用程序兼容性工具包 (act30pkg.exe) 来对系统进行全面校验。该工具包提供了使检查过程更易于管理的工具，并且还可以为各种操作系统打包它们所必需的兼容性修补程序。下载工具包并完成安装，可以使用其中的“Application Compatibility Analyzer (应用程序兼容性检查器)”对系统的软件部分进行兼容性检查。不过该工具必须在安装了 Service Pack 3 的 Windows 2000 中才能安装。

2. 备份重要文件

尽管在从 Windows 2000 Server 升级到 Windows Server 2003 的过程中一般不会破坏硬盘中原有的数据，但为了防止意外的发生，还是建议大家对重要文件进行必要的备份。

3. 查看日志中的错误信息

了解原系统中曾经发生或重复发生的系统错误，可以对在升级过程中可能出现的错误做到心中有数。在桌面上用鼠标右键单击“我的电脑”，在弹出的快捷菜单中执行“管理”命令，打开“计算机管理”窗口。在左窗格中展开“事件查看器”目录，并单击选中其中一项子目录即可在右窗格中查看到详细信息。



查看错误信息

4. 断开与UPS设备的连接

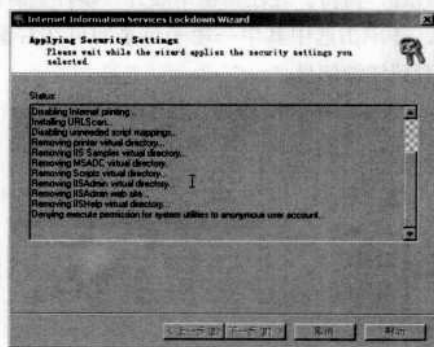
如果在准备升级的计算机上连接有 UPS（不间断电源）设备，应该在运行安装程序以前断开计算机与 UPS 设备的串行电缆的连接。这是因为安装程序会自动尝试检测连接到串行端口的设备，并且 UPS 设备可能会导致在检测过程中出现问题。

5. 升级期间禁用 IIS 万维网发布服务 (WWW 服务)

为防止服务器受到恶意用户的攻击，升级期间将禁用万维网发布服务 (WWW 服务)。默认情况下 Windows 2000 Server 会安装“Internet 信息服务 (IIS)”并要求管理员保护 IIS 以防止遭受攻击。当然如果不希望禁用 WWW 服务，则必须下载并运行 IIS 锁定工具 (IISlockd.exe)，或添加替代注册表项。否则，可以继续升级并在升级结束后重新启用 WWW 服务。



如果使用万维网发布服务（WWW 服务），强烈建议用户在升级到 Windows Server 2003 家族产品之前运行 IIS 锁定工具。IIS 锁定工具通过禁用或删除在 Windows 2000 Server 安装中出现的不必要功能以帮助保护计算机安全。IIS 锁定工具通过禁用不必要的功能而减少了表面攻击，并允许用户决定为站点启用的功能。否则，这些功能将在升级后保留在用户的机器上，使服务器易于遭受攻击。使用 IIS 锁定工具而不是在安装后使用替代注册表项或重新启用 WWW 服务，可使用户根据特定需要微调安全级别。



安装IIS锁定工具

11.2.2 开始升级系统

可以将从 Windows 2000 Server 升级到 Windows Server 2003 的过程总体上分为两步，即准备活动目录和升级主系统。

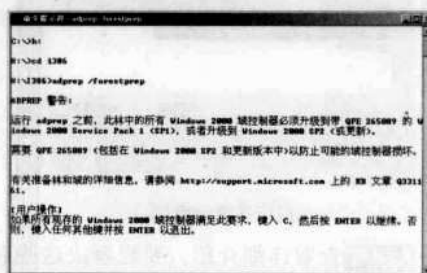
1. 准备活动目录

在将运行 Windows 2000 Serve 的域控制器升级至 Windows Server 2003 或者在第一个运行 Windows Server 2003 的域控制器上安装 Active Directory 之前，必须确保已经准备好服务器、林和域。在“架构操作主机”和“结构操作主机”上分别使用“adprep”命令来准备林和域，其中的域控制器就是“架构操作主机”。这个过程包括检查服务器的升级兼容性、准备林和准备域，可以使用系统提供的命令来完成这些工作。上文已经详细介绍了检查服务器的升级兼容性的方法，因此这里主要谈谈准备林和准备域的方法。

(1) 准备林

将 Windows Server 2003 安装光盘放入光驱，然后依次单击“开始 / 程序 / 附件 / 命令提示符”，打开“命令提示符”窗口。

在“命令提示符”窗口中将当前目录定位至 Windows Server 2003 安装光盘的“i386”目录下，然后键入命令行“adprep /forestprep”并回车，稍等片刻之后显示出提示信息。



执行adprep命令

注意

在运行 adprep 命令之前，此林中的所有 Windows 2000 Server 域控制器必须升级到带“QFE 265089”的 Windows 2000 Service Pack 1 (SP1)，或者升级到 Windows 2000 SP2。因为“QFE 265089（包括在 Windows 2000 SP2 和更新版本中）”可以防止可能的域控制器损坏。

接着键入命令“C”并回车，系统加载需要修改的各种项目并自动完成修改。经过一段时间以后，全林性信息被得到更新。



成功更新全林性信息

(2) 准备域

第十一章 网络升级与优化实战

当准备林的数据复制了整个林后，就可以为升级到 Windows Server 2003 准备域了。域准备操作必须在林中每个域的“结构操作主机上”执行，在这里域控制器担当了“结构操作主机”的角色。在“命令提示符”窗口中键入如下命令行“adprep /domainprep”并回车，稍等片刻之后即可显示成功更新了全域性信息。



更新全域性信息

注意

在使用 adprep 工具准备林和林中的域之前，不能将运行 Windows 2000 Server 的域控制器升级至 Windows Server 2003，或者将运行 Windows Server 2003 的域控制器添加到 Windows 2000 域中。

当准备域的数据复制了整个域后，通过运行 Windows Server 2003 安装光盘上的“i386\winnt32.exe”命令来升级域控制器，实际上这些操作将在升级主系统的过程中完成。

2. 升级主系统

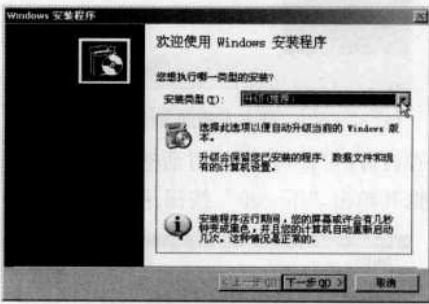
准备好活动目录后，就可以升级主系统了。在 Windows 2000 Server 的运行状态下将 Windows Server 2003 的安装光盘放入光驱，安装光盘自动运行并显示提示信息。为了保证设置后的 Windows 2000 Server 机器已经完全被 Windows Server 2003 所兼容，建议再次运行系统兼容性检查程序，以确认当前系统的兼容性情况。

然后依次单击“完成 / 上一步”回到首界面。在首界面中单击“安装 Windows Server 2003, Enterprise Edition”按钮。



安装Windows Server 2003

在随后打开的“Windows 安装程序”对话框中确保“安装类型”下拉框中为“升级（推荐）”选项，并单击“下一步”按钮。



选择升级安装

在“许可协议”选项卡中点选“我接受这个协议”单选框，并单击“下一步”按钮。在“用户的产品密钥”选项卡中键入用户拥有的合法的 Windows Server 2003 安装密钥，并单击“下一步”按钮。

注意

在接下来的时间里会进行下载更新的安装文件、复制文件、升级域控制器等一系列操作，不过在升级过程中不会出现诸如用户信息、网络配置、服务等方面的设置提示，因此整个安装过程几乎无需用户干预即可自动完成，只是升级过程比较漫长一些。

3. 安装关键补丁程序

对于 Windows Server 2003 而言，目前较为关键的补丁程序依然当属“冲击波”补丁和“震荡波”补丁，因此在安装系统后必须安装这两个补



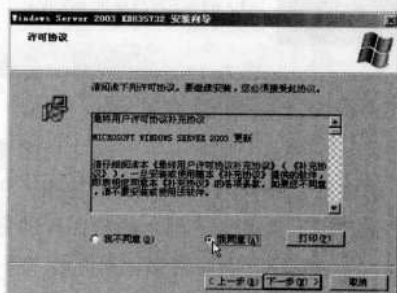
丁程序。针对 Windows Server 2003 开发的“冲击波”和“震荡波”补丁程序免费提供给用户，用户可以通过多种途径获得。以安装“震荡波”补丁为例，安装步骤如下：

执行“震荡波”补丁安装程序“WindowsServer2003-KB835732-x86-CHS.EXE”，经过验证和提取文件进入程序安装向导。单击“下一步”按钮。



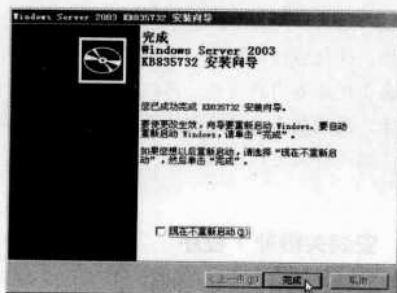
进入安装向导

在打开的“许可协议”对话框中，点选“我同意”单选框并单击“下一步”按钮。



同意安装许可协议

安装程序开始安装并更新系统文件，最后单击“完成”按钮重新启动电脑。



完成安装

安装“冲击波”补丁程序的方法跟安装“震荡波”补丁完全相同，这里不再赘述。

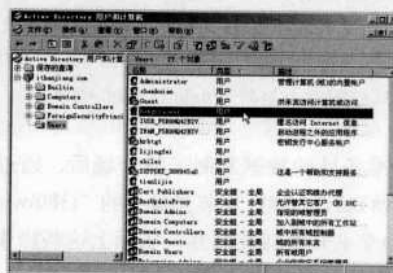
11.2.3 验证升级效果

现在服务器已经从 Windows 2000 Server 升级到了 Windows Server 2003，那么升级后的系统是否正常、是否达到了升级的目的还需要通过一些验证来获得答案。

1. AD 验证

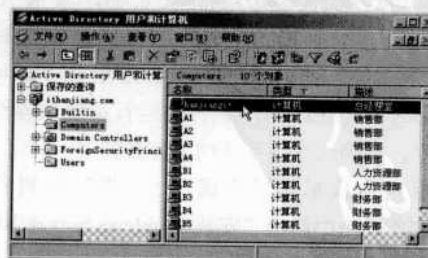
首先来验证一下比较敏感的 AD 升级效果，主要是看看升级后的用户数据是否完好，以及用户能否从工作站顺利登录到域中。

(1) 在升级后的 Windows Server 2003 服务器中依次单击“开始 / 管理工具 / Active Directory 用户和计算机”，打开“Active Directory 用户和计算机”窗口。在左窗格中依次展开“ithanjiang.com (域名) / Users”目录，可以看到在原来的 Windows 2000 Server 域中创建的用户列表，这说明用户的属性信息已经完整迁移到了 Windows Server 2003 域中。



验证域用户账户

(2) 在左窗格中依次展开“ithanjiang.com (域名) / Computers”目录，查看一下原来的域中的计算机是否成功迁移到了升级后的域中。



验证计算机账户

第十一章 网络升级与优化实战

(3) 以普通域用户的身份登录升级后的 Windows Server 2003 域，检验是否能够正常登录以及登录成功后在域中的权限是否改变。

2. 功能提升验证

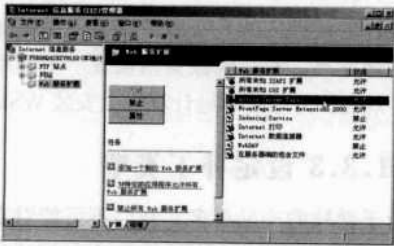
服务器升级至 Windows Server 2003 以后在活动目录、IIS、远程管理等方面都有了比较大的功能提升，下面对这些提升后的功能略窥一二。

(1) 活动目录

在 Windows Server 2003 的活动目录中增加了一些管理功能来简化部署过程，例如增加了跨森林信任关系、域重命名和构架撤销功能，从而弥补了 Windows 2000 Server 活动目录的不足。其还改进了很多用户界面，包括拖曳功能、多个对象选择和编辑以及保存查询的功能。另外提供的一套基于活动目录的命令行工具为习惯于命令行操作的管理员提供了更多的便利。

(2) IIS

随 Windows Server 2003 一起升级安装的 IIS 6.0 是 IIS 5.0 的升级版本。跟 IIS 5.0 相比，IIS 6.0 的运行速度要快很多，并且在安全性、可靠性和可管理性等方面都有了不小的进步。IIS 6.0 全面支持 .NET 架构，提供了出色的 ASP.NET 运行环境和 Web 应用程序开发机制。在默认安装的情况下，Windows Server 2003 未安装 IIS 并取消了默认的“运行”权限。IIS 6.0 的基于 XML 的配置数据库 (Metabase) 可以让使用任何一种基于 XML 的编辑器或文本编辑工具在线编辑并立即生效，而此过程无需重新启动服务器。

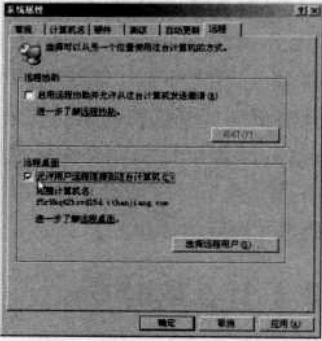


IIS 6.0对Web扩展服务的支持

(3) 远程管理

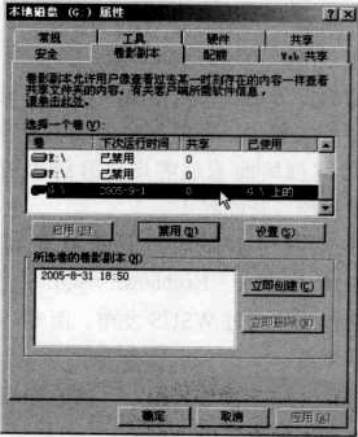
“远程桌面连接”是 Windows Server 2003 中增加的一项重要功能，为远程管理工作带来很大

帮助。其实在 Windows 2000 Server 中提供的“终端服务”同样可以实现远程桌面连接，只是配置起来稍显麻烦。而 Windows Server 2003 的远程桌面连接只需打个对勾就行了。



启用“远程桌面”功能

当然，升级到 Windows Server 2003 以后所获得的功能提升并不仅限于上述三种，像流媒体服务、卷影子副本服务 (VSS, Volume Shadow Copy Service) 等诸多功能有待用户去深入挖掘。



启用“卷影副本”服务

11.3 架设局域网升级服务器

如果不及时安装操作系统的补丁，会带来什么后果呢？冲击波、震荡波的厉害之处，想必大家都领教过了。因此及时更新操作系统的漏洞补丁，目前已成为提高系统安全性的主要手段。

然而，你会发现使用 Windows 自带的 Update



下载补丁，速度比较慢。如果你所在的公司内网中的员工计算机不能上网，你又该如何为大家打补丁呢？恐怕使用默认的 Update 是无法实现的吧。

现在，我们可以利用微软提供的 WSUS(Windows Server Update Services) 建立一个内部 Update 服务器，让公司内网中的计算机直接到这台 Update 服务器上下载补丁，以缩短用户打补丁的时间，及时提高计算机和网络的安全性。没有连接 Internet 的计算机只要在内网中能顺利访问 Update 服务器，也可实现随时打补丁，有效地防止漏洞型病毒在内网中传播。

11.3.1 什么是WSUS

WSUS(Windows Server Update Services) 是微软公司继 SUS(Software Update Service) 之后推出的替代 SUS 的产品。

软件平台：Windows Server 2000/2003

下载地址：<http://download.microsoft.com/download/9/3/3/933eaf5d-f2a2-4a03-8a87-e8f6e6d07e7f/WSUSSetup.exe>

使用过 SUS 的网管都知道，虽然可用它建立自动更新服务器，不过配置很麻烦，更新补丁的产品种类也较少，同时在实际使用中经常会因为网络带宽拥堵而造成客户机升级失败。那么 WSUS 具有哪些特性呢？

- 支持对更多微软产品进行更新，除了 Windows 外，Office、Exchange、SQL 等产品的补丁和更新包都可通过 WSUS 发布，而 SUS 只支持 Windows 系统。

- 提供了中文操作界面，以前的 SUS 操作界面为英文，不便于操作。

- 比 SUS 更好地利用了网络带宽。

- 对客户机的管理更强大，可针对不同客户机分配不同的用户组，并分配不同的下载规则。

- 在设置和管理上比 SUS 更简单直观。

硬件要求：如果网络中要升级的客户端计算机少于 500 台，架设 WSUS 服务器的硬件至少得是 750MHz 主频的处理器以及 511MB 内存，当然还需要充足的硬盘空间来保存更新程序的安装文件。

❖ 228 ❖

笔者所在公司的网络处于教育网之中，客户机连接微软官方的 Update 站点速度很慢，更新补丁的时间较长。为了提高公司网络的安全，加快补丁更新速度，笔者打算选择一台服务器通过 WSUS 建立一个公司内部的 Update 站点，让所有员工计算机到这个 Update 站点更新补丁，服务器名称为 softer。

准备工作：由于软件需要很多必备组件，如果在 Windows 2000 Server 上安装 WSUS 则需要安装这些组件，不过这些组件都是默认安装在 Windows Server 2003 上的，所以笔者建议大家使用 Windows Server 2003 部署 WSUS 服务器，同时建议大家不要在该服务器上安装其他 Web 网站。

11.3.2 安装WSUS

安装 WSUS 之前，先要保证 WSUS 必需的硬件条件，还要安装相应的组件，如 IIS 等。

在 Windows Server 2003 中没有启用 IIS 服务，所以我们需要安装“应用程序服务器”组件，并把 IIS 添加到本地计算机。下载 WSUS 并双击安装程序，程序将会自动解压缩。

现在，开始安装 WSUS，所有步骤和安装普通软件一样。在出现选择安装路径的界面时，需要注意的是，安装空间必须要有 6GB，而且所在驱动器必须是 NTFS 格式的文件系统。如果大家的 Windows Server 2003 中没有安装 SQL Server，那么该软件还会在计算机上安装 SQL Server 桌面版。

网站选择窗口时选择“使用现有 IIS 默认网站”即可，如果本地计算机还开启了其他站点服务。由于架设的是独立的升级服务器而不是其他服务器的镜像站点，在“镜像更新设置”中不用进行选择。现在，开始在本地计算机上安装 WSUS。

11.3.3 设定补丁类型

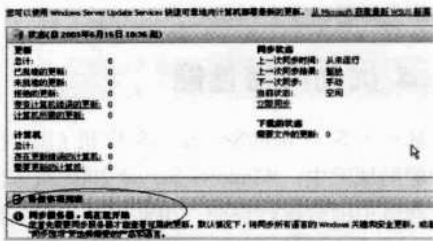
由于微软的产品很多，我们不可能对它的所有产品都进行更新，所以需要根据公司的实际情况对补丁的类型进行设置。

WSUS 安装完毕后，打开浏览器，使用地址 <http://localhost/wsusadmin> 访问 WSUS 的管理界面，

第十一章 网络升级与优化实战

也可直接输入计算机名或 IP 地址进行访问，在这里笔者输入 http://softer/wsusadmin 进行访问。输入 Windows Server 2003 系统的管理员账户和密码即可成功登录 WSUS 服务器。

第一次成功登录 WSUS 的界面后，会在下方“待做事项列表”中看到“同步服务器，现在开始”的提示信息，点击该选项开始设置 WSUS。



开始设置 WSUS

在同步选项设置界面，供我们设置的参数较多，由于篇幅有限这里不详细讲解了。平常用到最多的是“计划”下的“手动同步”或“每天定时同步”，一般情况下设置为“每天定时同步”。另外还有“产品和分类”下方的设置，我们可以在产品处选择可供更新的产品种类，除了 Windows 外，还有 Office、Exchange、SQL 等产品的补丁和更新包都可以通过 WSUS 发布。在“更新分类”处可以详细设置提供下载的补丁类别。

设置“产品和分类”与“更新分类”后，我们还要选择更新的语言种类，在同步选项设置界面的最下方有一个“高级同步选项”，通过它可以设置更新的语言为简体中文。

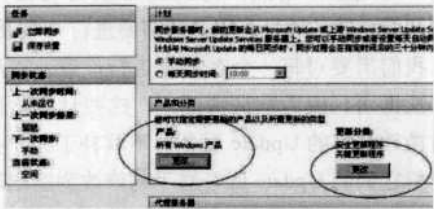
至此，便完成了补丁类型及语言的设定工作，所有的前期工作已告一段落，接下来就需要对服务器和客户机进行具体操作了。

11.3.4 下载并审批补丁

我们如何将相应补丁从微软网站下载到服务器上供公司内部计算机更新呢？这就需要下载并审批补丁。

在下图所示界面的左侧点击“立即同步”将启动服务器的同步功能，服务器将连接微软官方 Update 服务器下载相应补丁。补丁类型已经在设定补丁操作中进行了选择，服务器将只下载满足

设定条件的补丁，下载的补丁供客户端使用。在下载过程中我们不能进行任何操作，只能点击“停止同步”来结束更新操作。

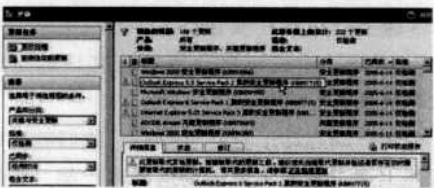


点击“立即同步”

大概等待 2 到 3 个小时就可完成补丁的更新，下载所用的时间是根据选择的补丁数量决定的。由于公司内网中的大部分计算机使用的都是 Windows 2000 操作系统，所以笔者只选择了更新 Windows 2000 补丁包及驱动程序。

仅仅下载完更新包还不能提供补丁更新服务，我们还需要对刚刚下载的“安全和关键更新”进行复查和批准，经过批准的补丁才能让客户端下载（实际上批准过程就是服务器对下载补丁进行检查的过程）。在待做事项列表中点击“复查安全和关键更新”。

在“更新”界面中可将所有补丁选中，选择完毕点击左侧“更新任务”栏中的“更改批准”，这样就会批准安装刚才下载的所有补丁。如果你不希望客户端下载某个补丁程序，则不选择该补丁。



点击“更改批准”

点击“更改批准”后会进入“批准更新”窗口，在批准下拉选项中选择“安装”，然后点击“确定”。现在，所有客户端就可下载并安装刚刚批准下载的补丁程序了，至此服务器上的所有设置完毕。

至此，服务器的设置操作就全部完成了，不过现在还要对客户端进行相应的设置，以使本来会使用 Windows Update 的客户端能够通过 WSUS 进行更新。



11.3.5 客户端设置

默认情况下客户机进行补丁更新都要到 Windows Update 站点，而我们希望将它修改为 WSUS 服务器的地址，因此还需要进行一些设置。

我们需要对每一个客户端进行设置，当然设置一次即可，因为默认情况下，这些计算机都是通过微软官方的 Update 服务器下载补丁的，我们需要将它们的 Update 服务器手动修改为刚刚建立的 WSUS 服务器。首先，在“运行”栏中输入“gpedit.msc”启动组策略（如果公司内部使用的是域建立的网络，那么直接在域控制器上设置组策略即可）。

依次点击“本地计算机策略→计算机配置→管理模板”，右键点击“管理模板”，选择“添加/删除模板”。通过“添加”按钮将 wuau 模板加入到“当前策略模板”中，添加这个模板后我们才能对 Update 站点信息进行修改。接着依次进入“本地计算机策略→计算机配置→管理模板→Windows 组件→Windows Update”，双击“配置自动更新”，然后选择自动更新补丁的类型，可以是手动更新也可以是自动更新。

接着在“Windows Update”中双击“指定 Intranet Microsoft 更新服务位置”，将刚刚建立的 WSUS 服务器地址添加进来。

最后，进入命令行模式，输入“wuauclt.exe /detectnow”命令启动更新，客户机就会立刻连接 WSUS 服务器下载并安装补丁。在组策略的“配置自动更新”中设定自动更新让客户端定时到 WSUS 服务器下载补丁。

当客户端启动了更新设置后，我们就可以在服务器上通过管理界面看到这些客户端。当然所有的补丁安装过程都是在后台进行的，我们在客户端上是不容易察觉的，要想了解客户端的补丁安装情况，只有通过服务器上的管理界面来查看。

11.3.6 部署成功

经过以上四个步骤，WSUS 的设置工作就算完成了，现在公司内部计算机都可使用配置好的 WSUS 服务器来更新多个微软产品的补丁，下载速度比连接官方站点快得多。而且，在实际使用

过程中，我们还可通过 WSUS 的分组设定功能将不同用户划分到不同的更新组，从而实现公司内部计算机补丁下载的权限管理。

自从采用 WSUS 搭建企业内部补丁更新平台之后，笔者发现公司员工的上网速度提高了，员工抱怨病毒骚扰的情况减少了，看来这一措施有效地防范了病毒、木马在公司内网中的扩散，公司网络变得更加安全和稳定了。

11.4 优化网络性能

基于 C/S (Client/Server, 客户机/服务器) 架构的局域网中，Windows Server 2003 服务器管理着网络中的软硬件资源。由此可见，服务器在网络中的地位非常关键，其性能的优劣直接影响着局域网的整体性能。与工作站相比，服务器的软硬件除了在保证应有的速度和性能的前提下，还应该具有高扩充性、高可用性、高稳定性以及独有的容错能力和冗余结构。但是高配置并不代表高性能，高性能的获得需要用优化硬件的工作状态和工作环境来换取。本节内容将谈一谈利用 Windows Server 2003 系统的自带功能和第三方软件两个大的方面优化服务器的具体方法。

11.4.1 系统自带功能优化

尽管采用 NT 核心的 Windows 2000 Server 系统的稳定性给用户留下了深刻的印象，不过如果能够在稳定性的基础上通过优化相关硬件设备的工作状态，从而使整个系统的性能有一个大的提升，又何乐而不为呢。Windows 2000 Server 自身带有一些调整软硬件工作状态和工作环境的功能，可以把这些调整分为“CPU 优化调整”、“内存优化调整”、“磁盘优化调整”和“网络接口优化调整”四项，所涉及的操作均不超出操作系统本身。

1. 内存优化调整

内存容量的大小对于服务器系统性能高低的影响自不必多言，尤其是对于那些需要承担大吞吐量数据流的服务器而言；增加内存的容量甚至比提升 CPU 主频更能明显提升服务器系统整体性

第十一章 网络升级与优化实战

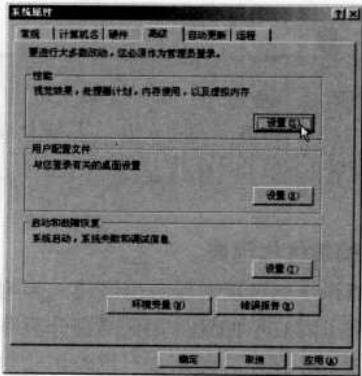
能。当然，如果用户并不希望为服务器进行额外的投入（尽管这样说对一个现代企业来说有多么牵强，但本例只是在讨论一项技术），那可以通过在操作系统层面对跟内存有关的参数进行一些调整，也可以在一定程度上提升服务器的整体性能。其实除了可以在 BIOS 中对内存的运行频率和延迟时间进行优化以外，还可以在操作系统层面调整页面文件的大小和位置、进行内存碎片的整理。

(1) 调整页面文件大小

在 Windows 2000 Server 中提到的页面文件实质上指的是虚拟内存，这是一块 Windows 2000 Server 用来同物理内存交换数据的磁盘空间。当物理内存空间不足时，Windows 2000 Server 的虚拟内存管理器就会将物理内存中较早读入的数据转移到页面文件上，把获得的空间分配给较新的程序使用，以缓和内存空间不足的问题。然而由于页面文件是建立在硬盘上的，尽管其充当了内存的角色，但是它的存取速度与物理内存相比相去甚远。所以对页面文件的优化将直接影响系统的性能。

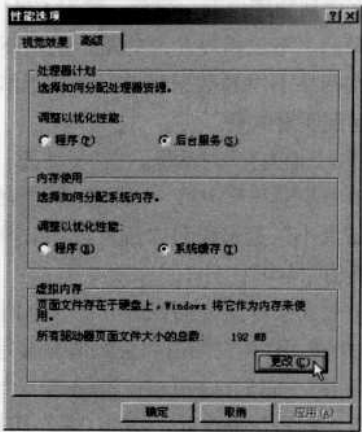
一般而言，页面文件的大小应该设置为物理内存容量的 2.5 倍左右。并且页面文件的最大值和最小值最好保持一致，这样可以减小硬盘损耗，也避免了大量磁盘碎片的产生。

STEP 1 打开“系统属性”窗口。在桌面上用鼠标右键单击“我的电脑”，执行“属性”快捷命令。在打开的“系统属性”对话框中切换到“高级”选项卡，并单击“性能”区域的“设置”按钮。



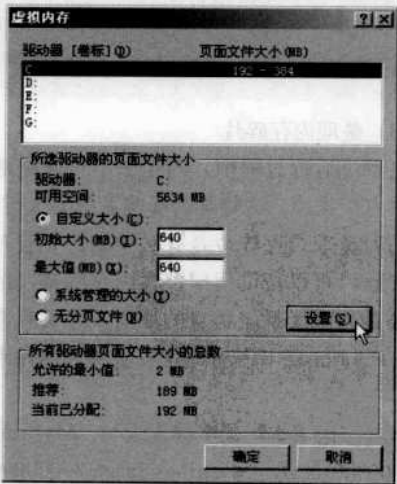
系统属性

STEP 2 打开“性能选项”。打开“性能选项”对话框，单击“虚拟内存”区域的“更改”按钮。



“性能选项”对话框

STEP 3 更改虚拟内存。打开“虚拟内存”对话框，因为本例中服务器的物理内存总容量为 256MB，所以根据“页面文件的大小应该设置为物理内存容量的 2.5 倍左右”的一般原则，在“初始大小”编辑框中键入“640”，并且在“最大值”编辑框中也键入“640”。单击“设置”按钮确定更改，依次单击“确定”按钮完成设置，并重新启动服务器使设置生效。



设置虚拟内存大小

(2) 调整页面文件位置

如果将页面文件设置在操作系统所在硬盘以



外的第二块硬盘，操作系统就可以在将物理内存中的数据转移到页面文件的同时，加载新的应用程序或文件到物理内存。显然，这对 CPU 的利用率是很高的。不过需要注意的是，两块硬盘必须分别接在两条不同的数据线上，否则所作的调整将无法起到明显效果。

打开“虚拟内存”对话框。在“驱动器 [卷标]”下拉菜单中找到并选中第二块硬盘驱动器的盘符，在“初始大小”编辑框和“最大值”编辑框中分别键入数值“640”。

选中页面文件所在的原始分区（本例为“C”区），将页面文件的初始值和最大值都改为零，并单击“设置”按钮。这时可能会弹出一个“系统控制面板小程序”提示框，单击“是”按钮即可。依次单击“确定”按钮并重新启动服务器使设置生效。



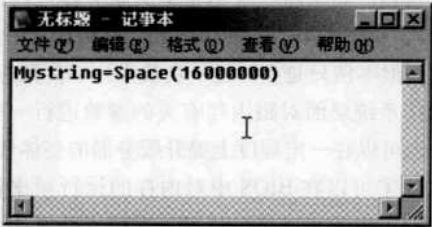
注意

如果从访问速度来考虑，系统文件和页面文件放在同一个分区可以减少磁头的调整，在性能上要优于将系统文件和页面文件放在同一硬盘的不同分区。因此如果服务器系统使用的是单硬盘，应该将页面文件保留在 Windows 2000 Server 的系统分区中。当然，双硬盘的情况属于例外。然而这样做的结果却会使系统分区产生过多的磁盘碎片，这似乎成了一个两难选择。

(3) 整理内存碎片

在系统运行过程中，内存中不可避免地会产生一些内存碎片，这势必会影响系统的执行效率，因此适时整理内存碎片是有必要的。尽管有许多第三方软件可以帮助用户整理内存碎片，但究其原理还是调用了系统本身的功能。其实只需借助一条 VBScript 脚本语句即可轻松实现内存碎片的整理。

打开“记事本”程序键入语句“Mystring=Space(16000000)”或“Mystring=Space(80000000)”。



输入语句

保存文件的时候，“保存类型”框应该选择为“所有文件”，“文件名框”中键入带扩展名“vbs”的文件名（例如“Memory.vbs”）。否则保存的文件将是一个文本文件。



保存为.vbs文件

在任何时间双击执行该文件都可以快速进行内存碎片的整理，尽管文件执行的时候没有任何提示，但内存碎片确实被整理了。建议在运行该文件时关闭其它应用程序，这样会得到最好的效果。



注意

上面的两条语句中，第一条语句适用于大于 32MB 但小于 118MB 的内存，第二条语句则适用于 118MB 及以上容量的内存。

2. 磁盘优化调整

存储系统的性能对服务器系统的影响同样不能被忽视，对它们的硬件优化是提升服务器系统性能的重要途径。一般而言可以把电脑中的存储系统分为内存和外存两个方面，上文谈了谈对内存

第十一章 网络升级与优化实战

存的优化，下面讨论一下对磁盘系统的优化调整。当然这些优化同样是在操作系统层面进行的。

在优化硬盘以前，首先保证将硬盘的跳线设置为“Master”（即主盘），并且还要保证使用UDMA/66 数据线将硬盘接到主板的 IDE1 接口上。除此之外，还应该在 BIOS 中将“IDE Primary Master”选项设置为“Auto”。此项设置允许在开机的时候自动侦测硬盘的 UDMA 功能并启用它。虽然系统的启动速度会因此而有所延迟，但这会大大提高硬盘的性能。

(1) 开启“Ultra DMA 66”支持

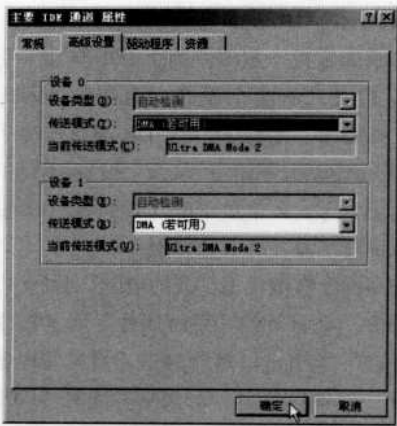
如果想要在 Windows 2000 Server 系统中充分发挥硬盘的性能，大家首先想到的肯定是开启硬盘的 DMA 功能。“Ultra DMA 66”提供最大 66Mb/s 的带宽，是“Ultra DMA 33”的两倍。尽管开启此项功能不会提高硬盘的读写速度，但它为硬盘提供了一条更快的数据传输通道。开启“Ultra DMA 66”的步骤如下所述：

在桌面上右键单击“我的电脑”，执行“属性”快捷命令。在打开的“系统属性”对话框中切换至“硬件”选项卡，然后单击“设备管理器”按钮打开“设备管理器”对话框。展开“IDE ATA/ATAPI 控制器”选项，右键单击“主要 IDE 通道”选项并执行“属性”快捷命令。



执行“属性”快捷命令

打开“主要 IDE 通道 属性”对话框。单击“高级设置”标签，在“高级设置”选项卡中保证两个设备的“传送模式”下拉列表中为“DMA（若可用）”模式，单击“确定”按钮。



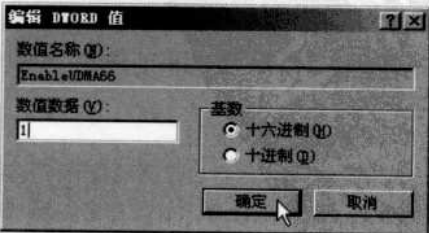
设置设备传送模式为DMA

依次单击“开始/运行”，打开“运行”对话框。在“打开”编辑框中键入“regedit”命令并单击“确定”按钮，打开“注册表编辑器”窗口。在左窗格中依次展开[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\0000]子键。右键单击“0000”子键，并依次执行“新建/DWORD 值”快捷命令。



新建DWORD值

在右窗格中将新建的键名“新值 #1”修改为“EnableUDMA66”，然后双击“EnableUDMA66”，将“数值数据”修改为“1”，并单击“确定”按钮。重新启动服务器使修改生效。



编辑DWORD值

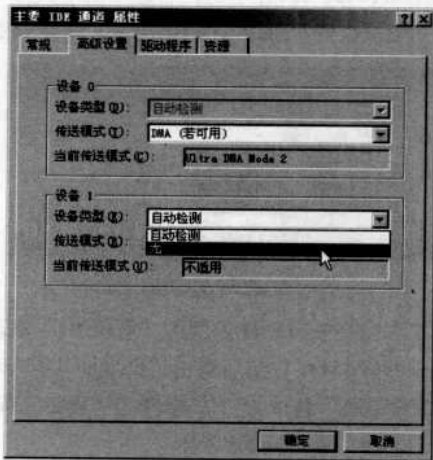


(2) 取消 IDE 空设备资源分配

目前的主板一般提供两个 IDE 接口，每个接口可以接主、从两个设备。而在 Windows 2000 Server 系统中，无论用户的 IDE 接口连接了几个设备，均会自动分配给主、从两个设备相应的资源。为了使硬盘等设备单独享用 IDE 的数据传输带宽，可以取消对空设备的资源分配。

在桌面上右键单击“我的电脑”，执行“属性”快捷命令。在打开的“系统属性”对话框中切换至“硬件”选项卡，然后单击“设备管理器”按钮打开“设备管理器”对话框。展开“IDE ATA/ATAPI 控制器”选项，右键单击“主要 IDE 通道”选项并执行“属性”快捷命令。

打开“主要 IDE 通道 属性”对话框。单击“高级设置”标签，在“高级设置”选项卡中首先确定空闲设备的设备号（设备 0 空闲还是设备 1 空闲）。本例中设备 1（即数据线上的从盘接口）是空闲的，在“设备 1”区域的“设备类型”下拉菜单中单击选中“无”选项，并单击“确定”按钮。



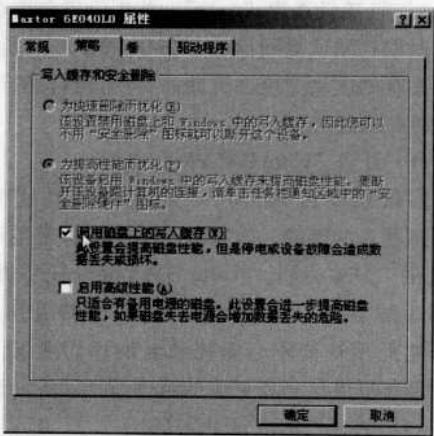
设置“设备类型”

重复上述步骤将“次要 IDE 通道”中的空闲设备类型同样设置为“无”。

(3) 开启磁盘写入缓存

开启磁盘的写入缓存会提高硬盘的读写速度，从而最大限度地降低磁盘系统给服务器系统带来的性能瓶颈。

打开“设备管理器”对话框，并展开“磁盘驱动器”选项。右键单击磁盘设备名称（本例中为“Maxtor 6E040L0”），执行“属性”快捷命令，打开“Maxtor 6E040L0 属性”对话框。切换至“策略”选项卡，选取“启用磁盘上的写入缓存”复选框并单击“确定”按钮。



启用磁盘写入缓存

3. 网络接口优化调整

服务器的网卡可以说是整个网络带宽的总出口，其性能优劣对网络的整体性能影响显著。目前的局域网大多升级到了 100M 的带宽，服务器所使用的网卡基本上全是 100M 或 10M/100M 自适应的。

为了避免由于网络接口的配置不当或没有发挥出网络接口的最佳性能而产生网络性能瓶颈，建议大家还是对网络接口进行必要的配置。例如可以将 100M 网络中的网络接口设置为 100M 全双工工作模式：

打开“设备管理器”对话框，并展开“网络适配器”选项。右键单击网卡名称（本例中为“Intel (R) PRO/100 VE Network Connection”），执行“属性”快捷命令。在打开的网卡属性对话框中切换至“高级”选项卡，在“属性”列表框中单击选中“Link Speed & Duplex”选项，并在“值”下拉列表中单击选中“100Mbps/Full Duplex”模式。最后单击“确定”按钮使设置生效。

第十一章 网络升级与优化实战



设置网卡传输速度

11.4.2 使用第三方软件

在上面的内容中讨论了利用操作系统本身具有的功能对服务器系统的关键硬件进行了一系列的优化设置。其实目前针对软硬件系统的第三方优化软件非常丰富，其中不乏优秀的工具软件。利用这些优化工具能够帮助用户方便、迅速地对服务器系统进行设置和优化，省去了很多繁琐的步骤。在众多的优化工具中，有针对某一硬件（如硬盘、内存等）进行优化设置的专门工具，还有一些全面优化系统的综合性软件。以综合性优化软件的优秀代表——“Windows 优化大师”为例，谈谈如何借助第三方软件对服务器系统进行全面优化。



注意

“Windows 优化大师”是国人自主开发的优秀系统优化软件，适用于 Windows 9X/2000/XP/Server 2003 操作平台。该工具可以为系统提供对诸如磁盘缓存、桌面菜单、文件系统、网络、开机速度、系统安全、后台服务等能够优化的参数或组件的优化服务，使系统始终保持最佳的工作状态。

1. 磁盘缓存优化

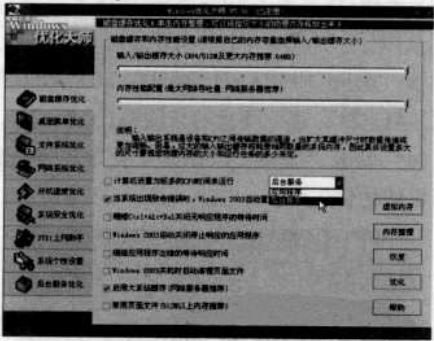
Windows 的磁盘缓存对系统的运行起着重要作用。一般情况下，Windows 会自动设定使用最

大量的内存作为磁盘缓存。为了避免 Windows 耗尽所有的内存作为磁盘缓存，用户有必要对磁盘缓存空间进行设定，从而保证其它程序对内存的需求。

(1) 启动“Windows 优化大师”，在左窗格中单击“系统性能优化”选项，打开下一级优化项目列表。然后单击“磁盘缓存优化”选项，打开“磁盘缓存优化”面板。

(2) 在右窗格中列出了详细的优化项目，其中顶端的滑块用来设置 Windows Server2003 的“输入/输出缓存大小”，拖动滑块可以看到“Windows 优化大师”根据机器的物理内存大小推荐的设置参数。本例所用服务器的物理内存总量为 384MB，因此将滑块拖动到了“64M”刻度线处。将“内存性能配置”项目的滑块拖动至最右侧，以适合服务器承担较大网络吞吐量的需求。

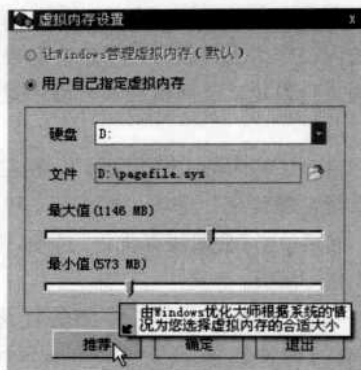
(3) 选取“计算机设置为较多的 CPU 时间来运行”复选框，并单击右侧的下拉三角，选取“后台服务”选项，这同样也是为服务器用户进行的优化。最后单击“优化”按钮完成优化，并重新启动计算机使设置生效。



磁盘缓存优化

2. 虚拟内存优化

虚拟内存的重要性在上述内容中已经有了详细介绍，在“Windows 优化大师”中同样可以灵活设置虚拟内存。在“磁盘缓存优化”面板中单击“虚拟内存”按钮，打开“虚拟内存设置”对话框。建议将虚拟内存设置在系统以外的硬盘上，并尽量采用“Windows 优化大师”推荐的大小。最后单击“确定”按钮。



优化虚拟内存

3. 文件系统优化

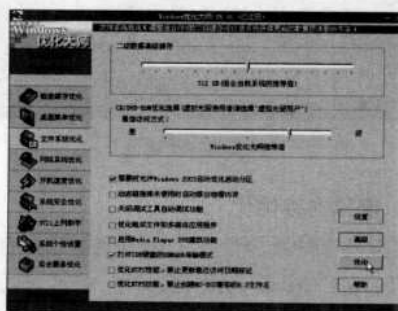
在“文件系统优化”面板中可以调整 CPU 的二级缓存大小，并调整光存储设备的最佳访问方式。

(1) 在左窗格中单击“文件系统优化”选项，打开“文件系统优化”面板。然后在右窗格中拖动顶端的“二级数据高速缓存”优化项目的滑块，将其置于“适合当前系统的推荐值”位置。

(2) 拖动“VCD/DVD-ROM 优化选择”优化项目的滑块，将其置于“Windows 优化大师推荐值”位置。

(3) 选取“打开 IDE 硬盘的 UDMA66 传输模式”复选框，优化硬盘的传输模式。

(4) 单击“优化”按钮完成设置，重新启动计算机使优化生效。



优化文件系统

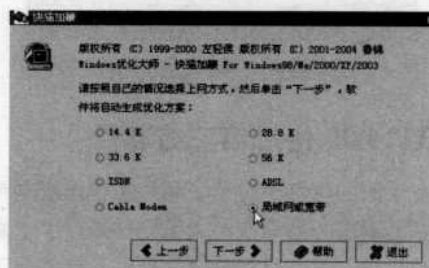
4. 网络系统优化

网络系统优化主要是根据 Windows Server 2003 接入 Internet 的方式来对某些参数进行调整，使

网络性能达到最优。

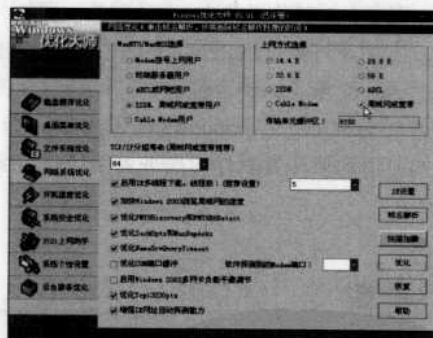
在左窗格中单击“网络系统优化”选项，切换至“网络系统优化”面板。在“上网方式选择”区域选择合适的接入方式（如“局域网或宽带”），在“MaxMTU/MaxMSS 选择”区域会自动选中“ISDN、局域网或宽带用户”单选框。

单击“快猫加鞭”按钮，打开“快猫加鞭”对话框。单击“下一步”按钮，在上网方式选择界面中点选“局域网或宽带”单选框，并依次单击“下一步/退出”按钮。



使用快猫加鞭

返回“网络系统优化”面板，单击“优化”按钮完成设置。重新启动计算机使优化生效。



优化网络系统



注意

MaxMTU（最大的 TCP/IP 传输单元）/MaxMSS（最大分组数）优化：Windows 默认的 MaxMTU 为 1500 字节（以太网标准），使用其它方式上网的用户采用 Windows 默认值会降低传输效率，例如，对于拨号用户 MaxMTU 一般应该设置为 576 字节，而 MaxMSS 应设置为 536。对此，Windows 优化大师提

第十一章 网络升级与优化实战

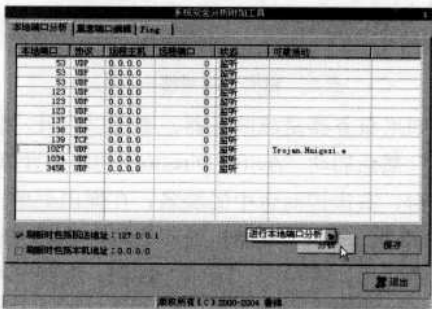
供了 Modem 拨号上网用户、终端服务器用户、ADSL 或网吧用户、ISDN/局域网/宽带用户、Cable Modem 用户等五种上网方式供用户选择设置。

5. 系统安全优化

安全问题似乎成了人们言必谈及的重要问题，因此“Windows 优化大师”也集成了针对安全问题的优化功能。

在左窗格中单击“系统安全优化”选项，打开“系统安全优化和设置”面板。然后单击“扫描”按钮，打开“安全检查”对话框。“Windows 优化大师”自动对端口进行扫描并报告扫描结果，弹出提示框后单击“确定”按钮即可修复存在的漏洞。

单击“附加工具”按钮，打开“系统安全分析附加工具”对话框。在“本地端口分析”选项卡中单击“分析”按钮可得到当前本地端口的连接情况，单击“保存”按钮可将本次分析所得到的日志文件保存为文本文件，以待日后分析使用。



分析本地端口



“系统安全优化”模块还提供了隐藏驱动器盘符、隐藏“控制面板”内的项目等诸多功能，对跟系统安全有关的设置考虑得很全面，用户可以根据实际需要设置。

6. 注册信息清理

在 Windows Server 2003 系统运行一段时间以后，注册表会不可避免地产生大量垃圾信息，这

势必会影响系统的运行效率。“Windows 优化大师”提供的“注册信息清理”功能可以帮助读者轻松完成清理工作。

在左窗格中单击“系统清理维护”目录，打开下一级选项列表。然后单击“注册信息清理”选项，打开“注册信息清理”面板。默认情况下“Windows 优化大师”已经选取了需要经常清理的信息项目，直接单击“扫描”按钮开始扫描。

扫描结束后，单击“全部删除”按钮。软件提示用户备份注册表信息，依次单击“是/确定”按钮即可删除无效的注册信息。



清理注册信息

7. 垃圾文件清理

“垃圾文件清理”也是需要经常进行的优化项目，通过该项操作可以及时清理掉大量临时文件和由于安装或卸载程序产生的垃圾文件。

在左窗格中单击“垃圾文件清理”选项，打开“垃圾文件清理”面板。选取需要扫描的驱动器盘符，单击“扫描”按钮开始扫描。扫描结束后单击“全部删除”按钮即可。



清理垃圾文件



11.4.3 优化网络结构

优化局域网另一个途径就是优化网络结构，其中包括优化布线系统已经划分 VLAN（虚拟局域网）等方面的操作。优化布线系统主要涉及按照国际标准（T568A 或 T568B）制作水晶头、网线的走线规则等，而划分 VLAN 则可以有效减少冲突域，提高网络通信效率。有关这两个方面的详细操作方法本书前面章节已经有所描述，这里不再赘述。

11.5 审核与日志管理

事件审核和系统日志的管理是服务器日常维护工作的一个重要部分。管理员通过设置审核特定的对象，然后在事件日志中就可以查找到某些账户的使用情况、服务器的安全问题和网络状况等信息。

11.5.1 审核策略的设置与应用

1. 启用审核策略的原则

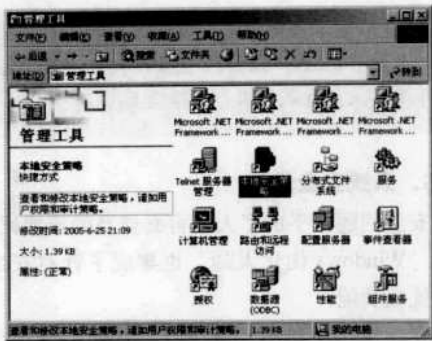
审核是必要的，但一定要注意不要妄图审查计算机上所有的事件。因为要审查的事件越多，日志就越大。而查看庞大的事件日志本身就是一件非常痛苦的事情，导致的结局甚至可能是不会再有人愿意看它了。

因此，在考虑审核事件时的策略非常重要，基本原则是应在不加重管理员负担的前提下适当的保护网络。另外需要注意的是，每增加一个审核事件，服务器就要增加一些执行上的消耗。

每次审核事件都要报告一些事情，但是这些有时并不是所需要的。如审查成功的登录和注销，可能会发现盗用密码，但它也会产生了很长只是记录正确授权用户正常登录和注销的事件。因此如果要审核是否有人进行随机测试破解密码，使用审核失败登录就能很清楚的得到这些事件的记录。

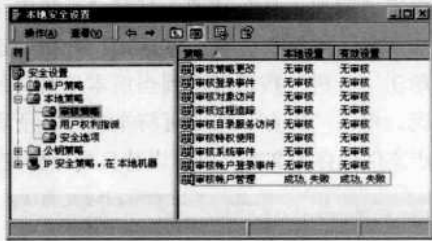
2. 启用审核策略的方法

登录系统后，依次双击打开“我的电脑→控制面板→管理工具→本地安全策略”。



选择“本地安全策略”

在打开的“本地安全设置”窗口中，依次展开“安全设置→本地策略→审核策略”项，在打开的右侧窗格中我们就可以打开相应的审核策略了。



查看审核策略

如果服务器是域服务器，则可以打开“管理工具”，然后启动“Active Directory 用户和计算机”控制台，右击控制台中的域名，在弹出菜单中单击“属性”命令；在弹出的对话框中选择“组策略”选项卡，再单击“编辑”按钮。在组策略控制台左边窗格上，依次单击打开“计算机配置→Windows 设置→安全设置→本地策略→审核策略”项，然后在右侧窗格中就能看到审核策略的内容。

系统提供了九项可以审核的事件，对于每一项都可以指明是审核成功事件、失败事件，还是两者都审核。

(1) 审核策略更改

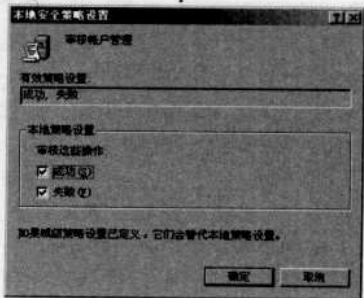
安全策略更改，包括特权指派、审核策略修改和信任关系修改。建议同时审核它的成功或失败事件。

(2) 审核登录事件

对本地计算机的交互式登录或网络连接进行审核。建议同时审核它的成功和失败事件。

第十一章 网络升级与优化实战

- (3) 审核对象访问
必须启用它以允许审核特定的对象（如某个文件夹的使用情况），建议审核它的失败事件。
 - (4) 审核过程追踪
详细跟踪进程调用、重复进程句柄和进程终止，这一项可以根据需要选用。
 - (5) 审核目录服务访问
记录对活动域的访问，如果有域服务，建议审核它的失败事件。
 - (6) 审核特权使用
记录某一特权的使用、专用特权的指派信息，建议审核它的失败事件。
 - (7) 审核系统事件
与安全（如系统关闭和重新启动）有关的事件、影响安全日志的事件。建议同时审核它的成功和失败事件。
 - (8) 审核账户登录事件
验证（账户有效性）通过网络对本地计算机的访问记录。建议同时审核它的成功和失败事件。
 - (9) 审核账户管理
记录创建、修改或删除用户和组，进行密码更改等操作。建议同时审核它的成功和失败事件。
- 要启用上述某个审核策略，可以双击该策略，然后在弹出的对话框中选择相应的复选框，设置是否开启该审核策略的成功或失败事件。各审核策略的开启原则是按需定制，如我们要对某些文件或对象的访问等事件进行审核，则可以开启“审核对象访问”或“审核目录服务访问”策略。



开启某个策略

按需定制好各审核项后，当有人尝试对你的系统进行某些方式（如尝试用户密码，改变账户

策略，未经许可的文件访问等等）攻击时，都会被安全审核记录下来，存放在“事件查看器”的“安全日志”中，从而帮助我们追踪攻击者的一举一动。

审核策略设置完成后，需要重新启动计算机才能生效。

3. 利用审核策略对机密文件或文件夹的访问进行审核

(1) 要对某个文件或文件夹的访问进行审核，首先要求审核的文件或文件夹必须位于 NTFS 分区内，其次必须如上所述开启“审核对象访问”策略。符合以上条件，就可以对该文件或文件夹的访问情况进行审核了，如哪些用户进行了哪些操作。



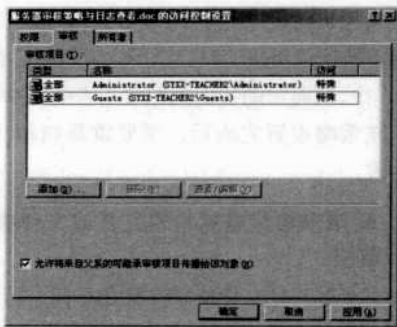
开启策略

(2) 右击要审核的文件或文件夹，然后选择“属性”命令，在打开的“属性”窗口中单击“安全”标签。



点击“安全”

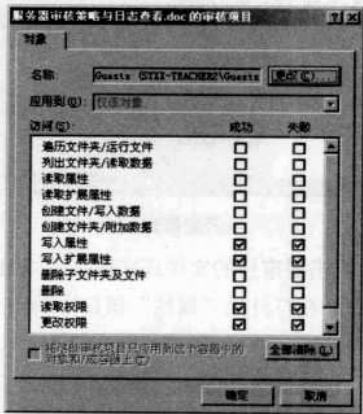
(3) 单击“高级”按钮打开“访问控制设置”对话框，切换到“审核”标签。



切换到“审核”

(4) 单击“添加”按钮，在“选择用户、计算机或组”对话框中选择想对该文件或文件夹访问进行审核的用户或用户组，单击“确定”按钮。

(5) 在“审核项目”对话框中，单击选择想要审核的事件后面的“成功”、“失败”复选框，选择完成后单击两次“确定”按钮关闭所有窗口，完成审核设置。



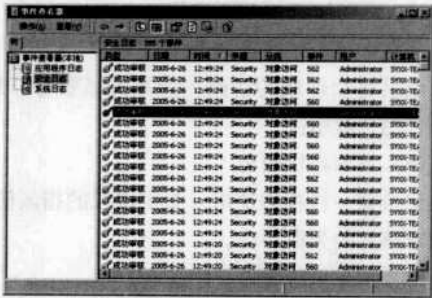
设置“成功”、“失败”



注意

这里要特别提醒各位的是，除非是非常重要的文件或文件夹才需要进行这样的审核，因为在设置该审核项目后在“事件日志”中会增加很多的条目，有时会把真正重要的问题掩盖起来，甚至丢失了。因此，在决定审核哪些事件的时候一定要仔细，审核的项目要尽量少，而且要确定该项目确实有审核的必要再加入。

(6) 设置了审核项目后，我们可以试着以审核用户的身份访问一下该文件或文件夹，并进行一下修改、删除等操作。然后打开“事件查看器”（在“控制面板”的“管理工具”中）的“安全日志”项，你就可以看到该用户刚才所做操作的事件记录了。



查看事件记录

11.5.2 系统日志管理与维护

1. 系统日志概述

通常的系统有三种日志：应用程序日志、安全日志和系统日志。配置为域控制器的 Windows 计算机还有另外两种日志：目录服务日志和文件复制服务日志；配置为域名系统（DNS）服务器的计算机还存在 DNS 服务日志；开启了 IIS 服务的计算机还有 FTP 日志、WWW 日志。根据系统服务的开启情况不同，系统中存的日志种类也会有所不同。



注意

常见日志文件的默认保存位置为：应用程序日志文件：%systemroot%\system32\config\App Event.EVT；安全日志文件：%systemroot%\system32\config\SecEvent.EVT；系统日志文件：%systemroot%\system32\config\SystemEvent.EVT；IIS 服务 FTP 日志默认位置：%systemroot%\system32\logfiles\msftpsvc1，默认每天一个日志；IIS 服务 WWW 日志默认位置：%systemroot%\system32\logfiles\w3svc1，默认每天一个日志。

系统日记可以记录的事件类型包括：用户和进程的登录和登出；对系统相关的数据和设备的

第十一章 网络升级与优化实战

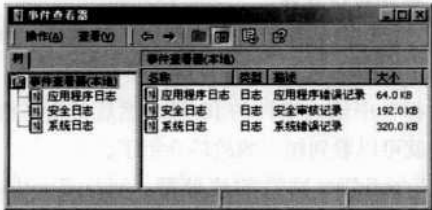
访问；改变用户帐号和用户组；改变对系统数据和资源的访问权限；关闭或重启系统，注册可信的登录进程，或者其它影响系统安全的活动；进程执行和跟踪；策略改变等等。

2. “事件查看器”的使用

“事件查看器”是系统自带的一款专门用来查看事件日志的工具，通过它可以查看操作系统组件、服务及应用程序等所发生的事件信息。当有事件发生时，用户就可以打开“事件查看器”来查看被记录下来事件的信息。这样可以使系统管理员由这些记录的信息得知系统的状态、错误发生的原因、用户的使用状况等，以便及时地发现和解决问题。

“事件查看器”可以显示的事件类型有：错误、警告、信息、审核成功和审核失败。显示的具体事件内容包括以下领域：数据、时间、用户、计算机、事件 ID、事件源（记录事件的软件，既可以是程序名，例如“SQL 服务器”，也可以是组件，例如驱动）、事件类型（事件严重程度分类：系统和应用程序日志中的错误、信息或警告；安全日志中的成功审核和失败审核，通过符号表示。）和事件种类（最初用于安全日志）。

双击打开“控制面板”中的“管理工具”，再双击“事件查看器”快捷方式就可以使用“事件查看器”这款工具了。

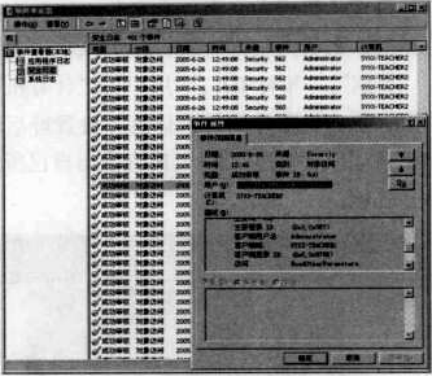


事件查看器

3. 查看“安全日志”寻找入侵痕迹

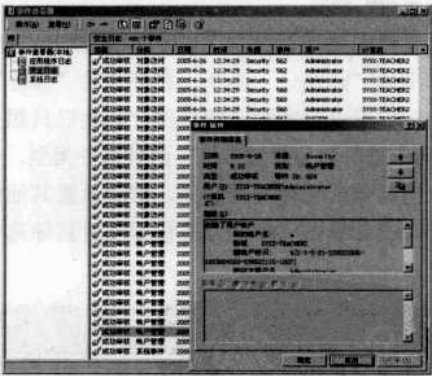
单击“事件查看器”下的“安全日志”项，在右侧的窗格中我们可以看到很多条的记录，比如我们前面提到的文件或文件夹审核记录，任意双击“对象访问”分类中的某条记录文件，就可以查看到更详细的内容，从图中我们可以看出

administrator 这个用户曾打开过这个文件。



日志记录

再如下图，从日志记录中我们可以看出，系统中被人新增了一个账号，账号名为 a，并且是 administrator 这个用户增加的。如果你的机器就你一人使用别无他人，那你可得小心了，是不是有人“逛”过了你的机器。再比如你在日志中发现了几个登录的失败审核，紧接着又出现登录成功的审核，那你可得仔细查看这些日志信息了，很有可能是你的密码太简单被人猜出来了，那就得赶紧增加密码的长度和复杂性了。



查看日志内容

4. 搜索、筛选日志，查找特定记录

当我们设置的审核策略不止一项时，日志中的各种信息就会混杂在一起，使得想查看特定的信息变得困难，这时我们可以使用“查找”功能在日志中进行搜索。

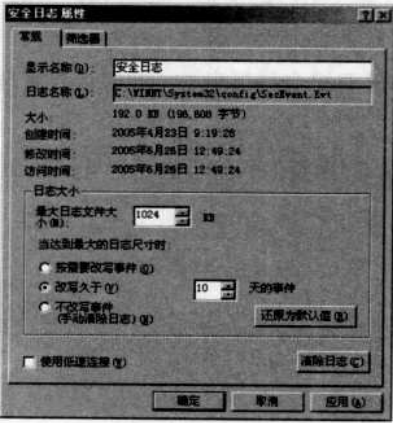
首先单击选择某类日志（如“安全日志”），

第十一章 网络升级与优化实战

6. 设定日志文件大小

随着审核事件的不断增加，安全日志文件的大小也会不断增加，默认情况下日志文件的大小是 511KB，当达到最大日志尺寸时，系统会改写 7 天以前的事件。

其实我们可以根据自己的需要对日志的大小进行更改，以更改“安全日志”为例，首先右击“安全日志”项，然后选择“属性”命令，打开“安全日志属性”窗口。在“常规”标签中，我们可以根据自己实际需要修改系统的这些默认设置，以满足自己存储安全日志的需要。



设置日志大小

7. 保存事件日志

如果用事件日志进行系统跟踪，那么就必须保存它们。从“设定日志文件大小”这项功能中，我们知道系统中的事件记录不可能无限制的被记录下来，要保存以前的事件记录，我们就得用“事件查看器”提供的存储功能了。这样我们就可以按需查看各时段的日志了。

首先选择要保存的日志类型（如系统日志），然后单击“操作”菜单下的“另存日志文件...”命令，最后在弹出的对话框中设置保存的文件名与文件类型（有 evt、txt、csv 三种格式）后单击“保存”按钮即可。

8. 修改日志文件存放路径

Windows 系统日志默认情况下被保存在 Windows 系统文件夹中，有的时候，如果你打算修改日志文件存放路径，可以通过修改注册表的方法。

(1) 修改“系统日志”存放路径

打开注册表编辑器，展开如下分支：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System，然后双击右侧窗格中的 File 键值，打开字符串编辑器。系统默认的存放路径是 %SystemRoot%\System32\Config\SysEvent.Evt，这时可以根据自己的需要设定新的存放路径。



修改存放路径

(2) 修改“应用程序日志”存放路径

打开注册表编辑器，展开如下分支：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application，双击并修改右侧窗口中的 File 键值即可，方法与前面介绍的相同。

(3) 修改“安全日志”存放路径

打开注册表编辑器，展开如下分支：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security，双击并修改右侧窗口中的 File 键值。

全部完成修改后，重新启动计算机即可使修改生效。

本章内容以网络升级和优化作为主要叙述内容，以大量可操作性的升级和优化步骤为内容表现形式，向读者展示了升级局域网和优化局域网性能的方法。通过阅读本章内容，读者将能对升级和优化局域网的方法和基本原则有一个初步的认识，并能独立完成升级和优化局域网的任务。

第十二章 服务器远程管理与维护

服务器除了机房环境调整，否则一般都是不动的。保持机房的清洁、无尘和良好的室温，是保证服务器寿命的重要前提。有经验的网管，大多都是通过远程管理服务器的方法，对服务器进行各种各样的配置。特别是一些托管机型，机主根本没有机会到机房去，此时远程管理就成了惟一能够使用的管理方式了。

就拿 Windows Server 2003 的多个远程管理功能来说吧，网管们利用这些功能至少可以实现

- > 用桌面模式或图形化界面访问远程计算机；
- > 远程安装、检测或修改应用程序；
- > 远程安装与卸载服务器组件；
- > 远程配置服务器环境；
- > 远程管理硬件，如安装打印机等；

.....

充分利用远程管理功能，可以极好地减轻网络管理员维护服务器的压力！比方说，网管下班回家后接到公司要求管理服务器的任务，他如果使用远程管理功能的话，就可以不慌不忙地在家对公司服务器进行管理，而不必再急忙赶往公司了！

12.1 远程桌面

利用 Windows Server 2003 的“远程桌面”功能，可以实现最简单的远程网络管理，网管可以用这项功能访问、检测与管理远程计算机。

12.1.1 什么是远程桌面

简单地说，“远程桌面”就是远程网络中的一台电脑的桌面，但从功能上来看，“远程桌面”则是一项极具实用性的远程管理功能，它允许网管在远程（如家里或外地）使用“远程桌面”功能连接到在公司的电脑上，进行所有应用程序、文

件和网络资源的调用操作，而这时公司里的那台电脑则可能仅仅只有主机灯在亮着，显示器却一片漆黑。

举个例子吧，网管正在进行着的服务器配置操作，到了下班时间后只好停止，这个时候通常情况下只能关闭计算机，等待第二天再继续工作。但实际情况却是，正在进行配置的服务器是不能随意关闭的，否则一切将会是前功尽弃，而且还可能会带来很多未知错误！这个时候，可以允许网管远程对服务器进行配置“远程桌面”功能就可以大显身手了，网管可以在下班之前，只关闭计算机的显示器，在不关闭主机的情况下，待回

第十二章 服务器远程管理与维护

到家后使用家中的电脑通过 Internet 和“远程桌面”功能连接到公司的服务器继续进行配置操作，这样既可以极大地提高了工作效率，又可以使服务器的配置不受丝毫影响。

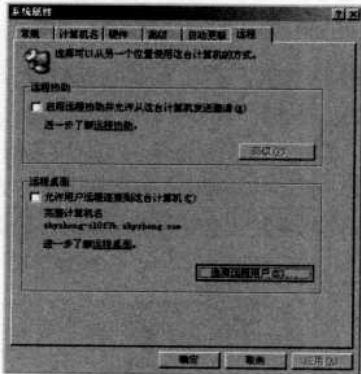
12.1.2 远程桌面所需条件

由于“远程桌面”功能需要两台电脑来运行，一台用于当作被控端，供用户远程使用，另一台用于当作访问端，用于远程访问被控端的电脑资源。所以要求：

- 有两台电脑；
- 两台电脑都能够连接到局域网或 Internet；
- 被控端电脑必需安装“远程桌面连接”功能。

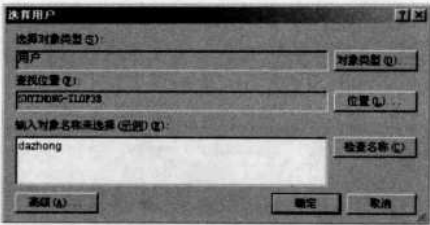
12.1.3 启用远程桌面功能

在“我的电脑”图标上单击右键，在弹出的快捷菜单中选择“属性”，在弹出的窗口中的“远程”选项卡设置界面中，选中“允许用户远程连接到这台计算机”项前的选框，并点击“选择远程用户”按钮。



点击“选择远程用户”按钮

在弹出的“远程桌面用户”对话框中可以看到 Administrator（默认管理员账户）默认状态下已经有了访问权，如果还需要添加其他账户的话，则应点击“添加”按钮，设置可以远程访问这台计算机的账号。在弹出的“选择用户”对话框中，既可以手工输入账户名（如 dazhong）后点击“确定”按钮完成操作。



“选择用户”对话框

也可以点击“高级”按钮，在展开的窗口中点击“立即查找”按钮，在当前系统中所有的用户都罗列出来后，选择一个带有密码的用户名并点击“确定”按钮即可。



当前系统的所有用户

点击“确定”按钮即可将上图中的“dazhong”用户添加到远程桌面控制组中了。

注意

为了安全，请一定要将选中的账户设置复杂的密码。此外，如果系统启用了防火墙功能，则需要在防火墙中开放“远程桌面”服务才行。

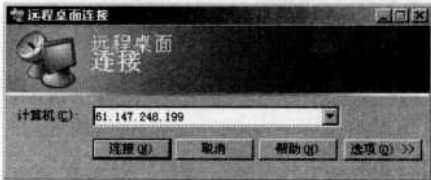
12.1.4 使用远程桌面功能

现在就可以进行远程电脑的登录及管理操作了。在 Windows Server 2003 中使用“远程桌面”功能进行远程登录的操作很容易，方法如下：

点击“开始→程序→附件→通讯→远程桌面连接”菜单项，弹出“远程桌面连接”对话框。



在“计算机”右侧的文本框中输入远程计算机的IP，当然也可以是局域网的IP，然后点击“连接”按钮。



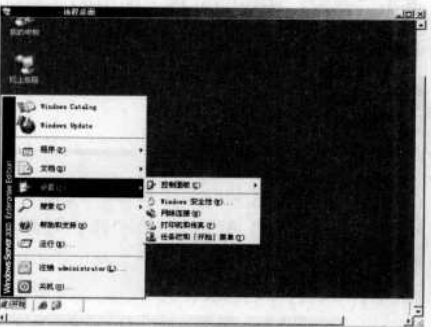
输入局域网的IP

在稍后弹出的窗口中，可以看到和本机登录Windows Server 2003 时一样的登录对话框，从中输入登录用户名和密码后，点击“确定”按钮。



输入登录用户名和密码

稍待片刻后，就可以登录到远程桌面了。



登录到远程桌面

这时被远程访问的计算机自动切换到登录界面，同时保持着当前账号的信息和所有已运行的程序（也就是说远程桌面功能不允许同时有两个用户同时登录，当远程用户登录后，本地用户将会被暂时挂起；当本地用户重新登录后，远程用

户则会自动断开）。



注意

远程运行被控端计算机中的程序速度，要受被控端计算机的本身速度、网络速度和控制端计算机的本身速度等几个方面的影响。如果出现稍慢的现象，这是正常的。

12.2 终端服务器

终端服务器作为 Windows 服务器中的标准组件，它可以使远程有权限的网络用户，通过桌面界面登录的方式对服务器进行管理。这种图形化的管理界面、强大的管理权限，都使终端服务功能得到了广泛肯定。更重要的是，使用终端服务器方式登录远程服务器，还可以解决使用“远程桌面”时只能一个用户登录的问题！

在本小节中，将以 Windows Server 2003 为环境，给读者讲述终端服务器的架设与管理。

12.2.1 什么是终端服务器

终端服务实际上就是 Windows 提供了一种“允许用户在远端执行 Windows 终端服务器上应用程序”的技术。终端服务通常由 5 个组件组成：多用户内核、远程桌面协议、终端服务客户端软件、终端服务许可服务以及终端服务系统管理工具。



终端服务器与远程管理员的连接

远程管理员对终端服务器进行连接、登录、程序应用等操作时，除了远程管理员进行的添加文件操作可以直接在终端服务器上显示，其他的操作将不会在终端服务器中有明显的显示。

如，客户端用户在终端服务器的桌面上新建了一个文本文件，那么终端服务器的桌面上将立

第十二章 服务器远程管理与维护

刻会显示出这个文本文件。而在客户端调用终端服务器的任何程序（包括桌面上的程序），都不会在终端服务器上进行实时的显示。这就给多用户同时对终端服务器进行操作提供了合理的桌面分配性。

12.2.2 终端服务器的建立

Windows Server 2003 的终端服务分别继承了 Windows 2000 和 Windows XP 终端服务的部分优秀功能，可以说是汲取了多家所长于一身。经改进的终端服务功能在 Windows Server 2003 中可以顺应各种情况。在许多可圈可点的改进设计中，有很多是值得深入研究的，如：重新定向来源端的文件系统、音效、串行端口等改进，在一定程度上使 Windows Server 2003 都成为了真正的多会话环境操作系统！

1. 终端服务器的安装

在 Windows Server 2003 中，安装终端服务器可以通过“配置您的服务器向导”来快速完成安装操作。

依次点击“开始→设置→控制面板→管理工具→配置您的服务器向导”菜单项，在弹出的“欢迎使用配置您的服务器向导”窗口中点击“添加/删除角色”。



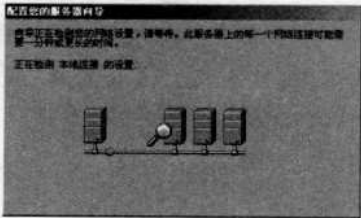
添加/删除角色

在稍后弹出的“预备步骤”中点击“下一步”按钮继续。



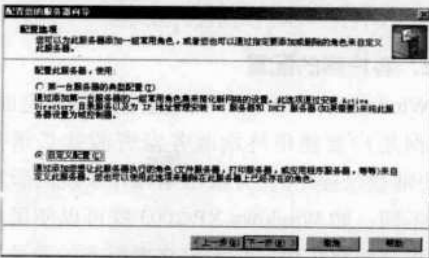
点击“下一步”按钮

接着向导会检查服务器的网络设置。此时请耐心等待。



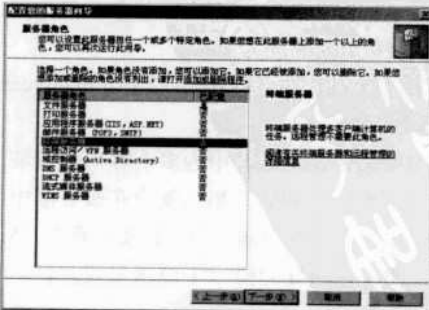
检查服务器的网络设置

待完成检查后，将会弹出“配置选项”窗口，选中“自定义配置”，并点击“下一步”按钮继续。



配置选项

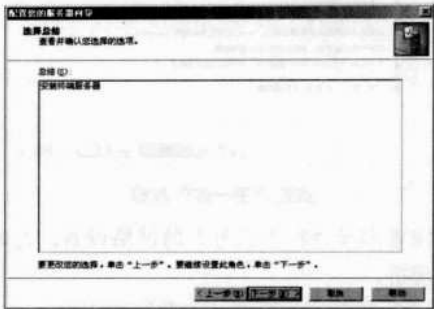
在下一步的“服务器角色”选择窗口，这里请选择“终端服务器”并点击“下一步”按钮。



服务器角色



接下来,在“选择总结”窗口中点击“下一步”,确认选择的选项需要安装。



确认选择的选项

完成对终端服务器的安装配置后,重新启动系统就完成了对终端服务器的快速安装。



注意

除了上述方法可以添加终端服务外,也可以使用“添加或删除程序”的方法来安装终端服务器。具体方法略。

2. 客户端的配置

Windows Server 2003 终端服务器安装完成后,局域网用户要使用终端服务器资源就必须安装“客户端登录程序”。方法根据操作系统的版本不同而不同,如 Windows XP/2003 就可以使用自身的远程桌面连接程序来完成终端服务的登录。而 Windows 98 则要使用专门的登录程序了,或是运行 Windows Server 2003 的客户端安装程序来生成登录组件。

以 Windows Server 2003 安装在 C 盘为例,客户端安装程序的路径为:

“C:\Windows\system32\clients\tsclient\win32”;

如果需要在局域网中为多个客户端安装“客户端登录程序”的话,那么就应在服务器中共享这个目录,这样客户端只须运行安装程序“Setup.exe”,便可在向导的提示下快速完成“客户端登录程序”的安装。



安装路径

3. 登录终端服务器

登录终端服务器的操作上,与使用“远程桌面”功能登录远程计算机的操作并无区别,登录后两者的显然状态也是一样的。只不过两者最大的不同就是可以同时登录的用户数量有所改变,“远程桌面”功能只允许一个用户登录远程系统,而“终端服务”功能则允许只要是有权限登录的用户,都可以同时登录终端服务器。

12.2.3 组策略与终端服务器

因为 Windows Server 2003 中对网络功能进行了诸多的权限设计,所以当 Windows Server 2003 中的终端服务出现这样或是那样的问题时,不妨尝试组策略中是否可以解决。

依次点击“开始→运行”,在弹出的“运行”对话框中输入“Gpedit.msc”命令打开“组策略编辑器”窗口。依次打开“计算机配置→管理模板→Windows 组件→终端服务”项,在右侧的窗口中可以看到组策略中有关于终端服务的设置选项。



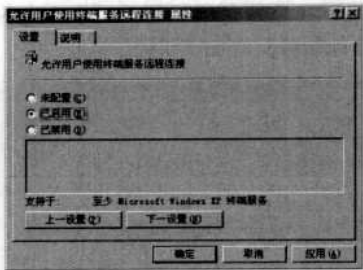
组策略设置栏

1. 允许远程用户访问

双击打开右侧的“允许用户使用终端服务远

第十二章 服务器远程管理与维护

程连接”项，弹出相应的对话框，勾选其中的“已启用”项后点击“确定”按钮。



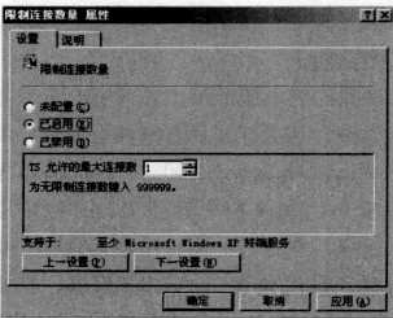
勾选其中的“已启用”项

如果将状态设置为“已启用”，则远程用户可以使用终端服务远程连接到终端服务器；如果将状态设置为“已禁用”，则终端服务器维护当前连接，但是不接受任何新传入的连接请求。

2. 限制连接用户数量

通过“限制连接数量”项，可以限制在终端服务器上可以同时连接的用户数量。如果超出指定数量，试图进行连接的额外用户将会收到错误信息，通知终端服务器正忙，稍后再试。这个选项至少有两方面的好处：一是可以大大保持系统的性能稳定性；二是可以很好地解决安全方面的问题。

双击“限制连接数量”项，在弹出的“限制连接数量 属性”对话框中点击勾选“已启用”项后，在随之呈可设置状态的“TS 允许的最大连接数”右侧设置数量为“1”。



允许的最大连接数设置

上述设置的作用是：只允许一个有权限的用户登录终端服务器。在这个设置生效后，如果合

法用户忽然发现自己登录不上终端服务器了，就应立即考虑是否被非法用户入侵终端服务器了。

12.2.4 终端用户权限的设置

虽然已经成功地安装了终端服务器，但它的默认设置不一定能满足局域网用户的需要，因此，还须根据用户的需要合理配置终端服务器。例如，在 Windows Server 2003 终端服务器的默认设置下只有少数用户可以登录到终端服务器，如管理员组用户、系统组用户等，而一般的局域网用户是不能使用终端服务器的，因此要在终端服务器上为这些用户添加相应的权限。

依次点击“开始→设置→控制面板→管理工具→计算机管理”菜单项，在打开的“计算机管理”窗口中展开“系统工具→本地用户和组→组”项，在右键选中“组”后单击，在弹出的快捷菜单中选择“新建组”。



新建组操作

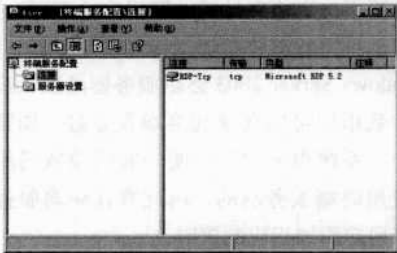
在稍后弹出的“新建组”窗口中的“组名”项右侧文本框中输入“lovebook”，点击“创建”按钮添加这个组。



“创建”按钮

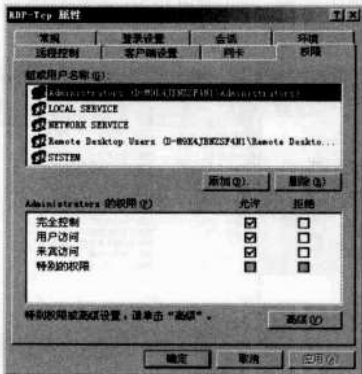


接着将所有要访问终端服务器的局域网用户都添加到该组中。然后在服务器端依次点击“开始→设置→控制面板→管理工具→终端服务配置”菜单项，在“终端服务配置”窗口的左栏中点击“终端服务配置→连接”项。



“终端服务配置”窗口

双击进入“RDP-Tcp”属性窗口，点击切换到“权限”选项卡设置界面，点击“添加”按钮。



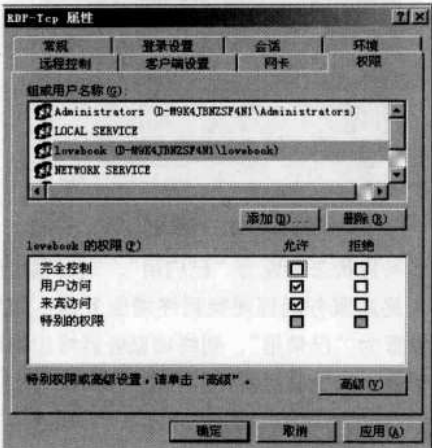
添加权限

进入“选择用户组或用户”窗口，点击下方的“高级”，然后点击“立即查找”，找到“lovebook”用户组，点击“确定”。



找到“lovebook”用户组

最后，在“权限”框下方的“lovebook 的权限”列表框中勾选“用户访问”和“来宾访问”的允许访问权限，这样就可以赋予“lovebook”用户组访问终端服务器的指定权限了。



终端服务器的指定权限

12.2.5 终端服务器的日志审核

当人们出海远行的时候，总是要做好航海日志，以便作为日后工作的依据。日志文件作为微软 Windows 系列操作系统中的一个比较特殊的文件，在安全方面具有无可替代的价值。

日志每天为我们忠实地记录着系统所发生一切，利用系统日志文件，可以使系统管理员快速对潜在的系统入侵作出记录和预测，但遗憾的是，目前绝大多数的人都忽略了它的存在。反而是因为黑客们光临才会使系统管理员想起这个重要的系统安全功能。

大多数的终端服务器上并没有打开终端登录的日志程序，其实打开日志审核是很容易的。

在 Windows Server 2003 中，依次单击“开始→设置→控制面板→管理工具→终端服务配置”菜单项，在打开的窗口中使用鼠标左键双击“连接”项右侧窗口的 RDP 服务，在出现的“RDP-TCP 属性”对话框中切换到“权限”选项卡设置界面。

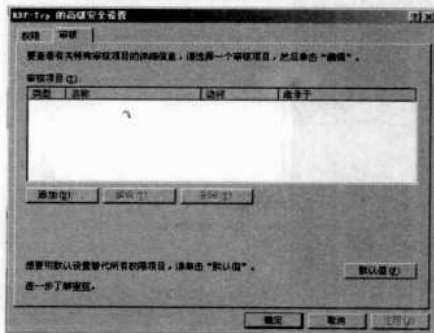
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十二章 服务器远程管理与维护



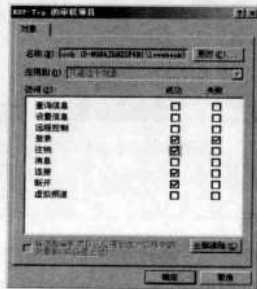
“权限”选项卡设置界面

接着单击下方的“高级”按钮，在弹出的对话框中单击切换到“审核”选项卡设置界面，单击“添加”按钮。



“审核”选项卡

接着在弹出的“选择用户和组”对话框中选择并添加“lovebook”组（根据实际情况选择所需组），然后审核其“连接→断开→注销”的成功和“登录”的成功与失败就足够了。



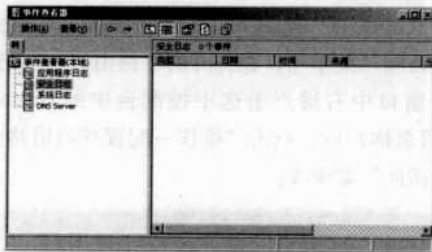
“选择用户和组”对话框



注意

记住审核选项不要选择太多，太多了反而不好，因为太多的审核将会产生海量信息，甚至有可能让硬盘爆满。

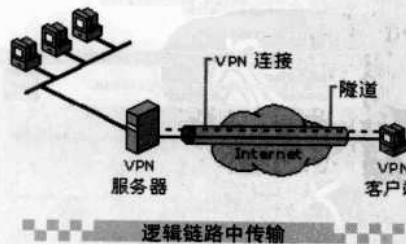
由于这个审核是记录在安全日志中的，所以管理员可以在“管理工具”里的“事件查看器”中查看到相应的信息。



事件查看器

12.3 配置VPN服务器

VPN 即“Virtual Private Network”的简称，中文是“虚拟专用网络”的意思。这是一项在公用网络上建立专用网络的技术。之所以称为虚拟网主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台（如 Internet, ATM, Frame Relay 等）之上的逻辑网络，用户数据在逻辑链路中传输。



由于通过公用 IP 网络来建立 VPN，这样就可以节省大量通信费用，可称得上物美价廉。

如果上述的解释还不能让大家明白，那么就再从解决实际问题的角度上看看 VPN 服务

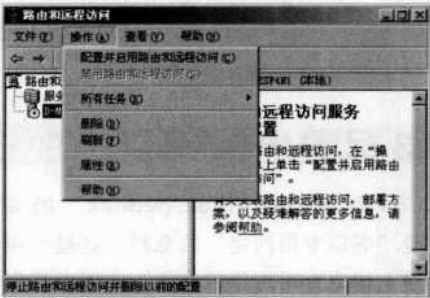


的作用。

假设 A 公司因业务扩展，在外地设立了 A1 分部。现在 A1 分部需要时时访问公司内部的网络，来查阅一些内部资料，那么这就是个“远程用户通过 Internet 访问 A 公司内部网络”的过程，显然“网络访问路径”需要两层，即 Internet 和内部网络。这个时候，就可以使用 VPN 服务来解决两层访问的问题了。下面让我们来看看如何配置：

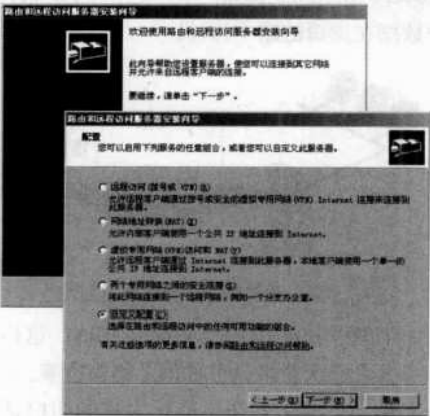
12.3.1 配置VPN服务器

依次点击“开始→程序→管理工具→路由和远程访问”菜单项，在打开的“路由和远程访问”服务窗口中右键点击选中控制台中的 Hostname（本机名称）后，点击“操作→配置并启用路由和远程访问”菜单项。



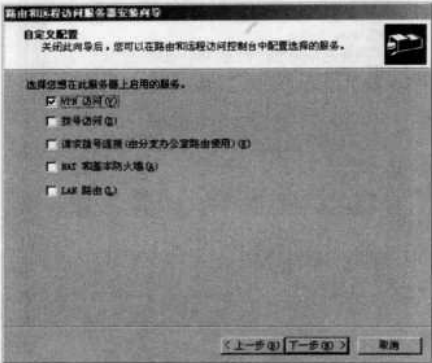
路由和远程访问

在稍后弹出的安装向导中单击“下一步”按钮，在“配置”对话框中选择“自定义配置”选项后继续。



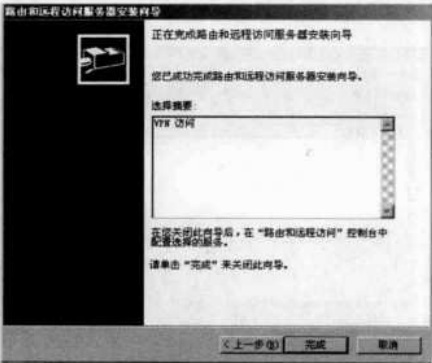
选择连接方式

接着在“自定义配置”对话框中勾选“VPN 访问”项后继续。



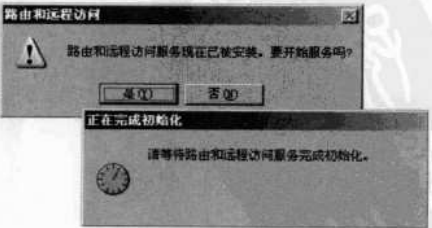
勾选“VPN访问”项

在下一步中点击“完成”按钮。



点击完成

在稍后弹出的“路由和远程访问”对话框中点击“是”按钮后，等待几秒钟后，待路由和远程访问服务完成初始化操作后 VPN 服务器即可启动了。



完成初始化

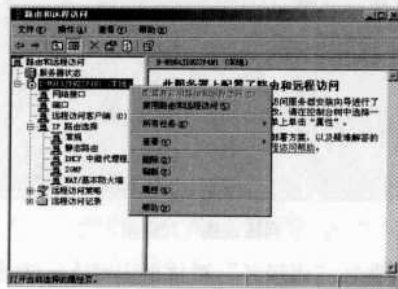
接着需要使用静态 IP 地址池为拨入端分配 IP 地址，这样可以减少 IP 地址的解析时间，从而有

Chapter

第十二章 服务器远程管理与维护

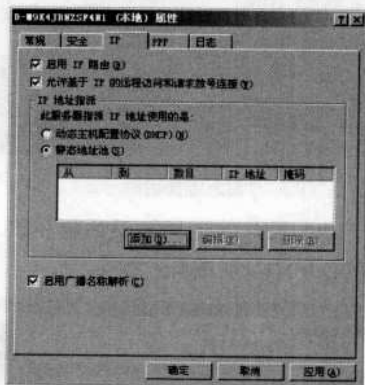
效提高远程连接速度。方法是：

右键选中并点击控制台中的服务器名，在弹出的快捷菜单中选中“属性”菜单项。



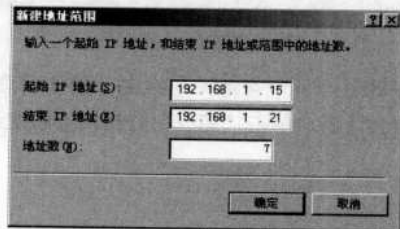
“属性”菜单项

在稍后打开的“hostname（本地）属性”窗口中点击切换至“IP”选项卡设置界面。在“IP地址指派”选项中点击选中“静态地址池”后，再点击“添加”按钮。



添加静态地址

在弹出的“新建地址范围”对话框中，在“起始 IP 地址”和“结束 IP 地址”右侧的 IP 地址栏中键入所需的内部网络的 IP 地址范围即可（如 192.168.1.15~192.168.1.21）。

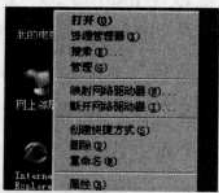


设置IP范围

12.3.2 添加权限账号

在服务器配置完毕后，还需要为远程的用户添加一个拨入 VPN 服务器的权限账号，VPN 服务器将使用该账户对远程连接进行认证。

右键选中并点击“我的电脑”图标，在弹出的快捷菜单中选择“管理”菜单项。



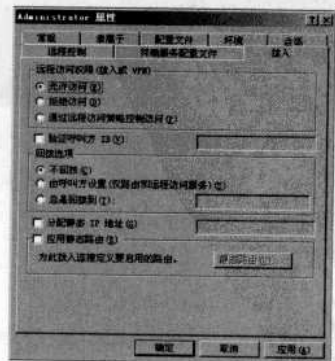
“管理”菜单项

在打开的“计算机管理”窗口中展开“本地用户和组→用户”项，使用右键点击用户列表中的某一个用户名称（如 Administrator），在弹出的快捷菜单中选择“属性”。



点选属性选项

在打开的“Administrator 属性”窗口中点击切换到“拨入”选项卡设置界面，点击勾选“远程访问权限”部分的“允许访问”选项。



选项卡设置界面



设置完毕后，点击“确定”按钮后就结束了服务器与账号的设置操作了。下面让我们来看看VPN客户端的配置方法。

12.3.3 配置VPN客户端

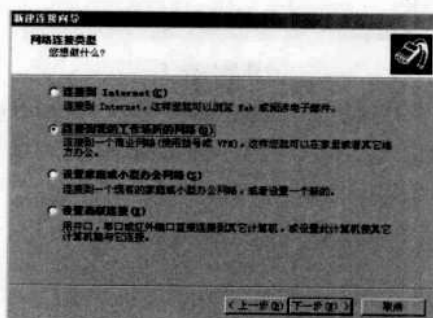
由于目前使用 Windows XP 系统的用户比较多，所以下面就以 Windows XP 操作平台为客户端环境，讲解一下 VPN 客户端的配置方法。

双击“控制面板”中的“网络连接”项，在打开的“网络连接”窗口中双击左侧“网络任务”区域的“创建一个新的连接”链接。



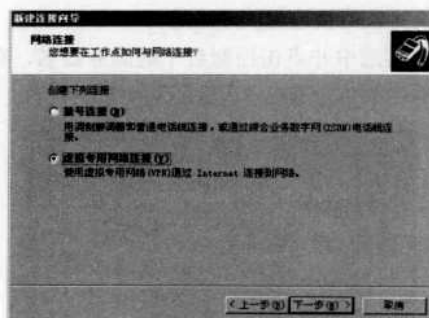
创建新连接

在弹出的“新建连接向导”进行到“网络连接类型”对话框时，点选“连接到我的工作场所的网络”选项继续。



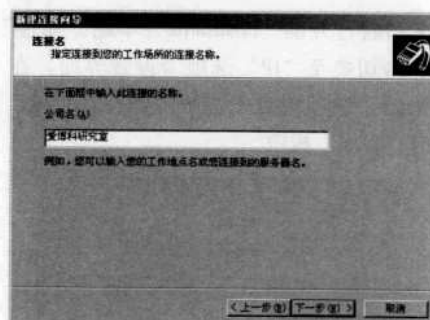
选择连接类型

在“下一步”的“网络连接”对话框中选择“虚拟专用网络连接”后继续。



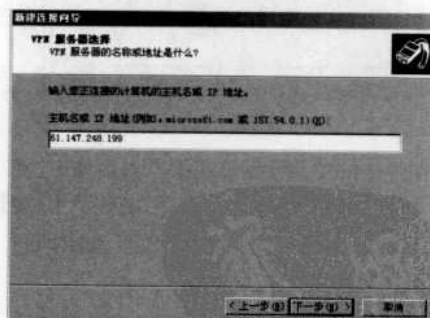
“网络连接”对话框

接着在“连接名”对话框中键入一个连接名称后继续。



键入连接名称

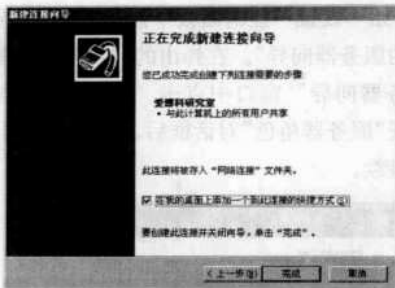
在“VPN 服务器选择”对话框中键入 VPN 服务器端的 IP 地址或域名后继续。



键入VPN服务器端的IP地址

在最后一步中勾选“在桌面上创建此连接的快捷方式”后，单击“完成”按钮结束创建过程。

第十二章 服务器远程管理与维护



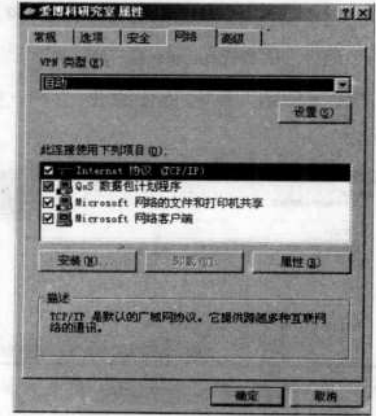
单击“完成”按钮

为了避免出现成功连接 VPN 服务器后，客户端不能访问 Internet 的问题，还需要对刚刚创建的“VPN 连接”做简单的配置。在“网络连接”窗口中右键单击“爱博科研究室”图标，在弹出的快捷菜单中选择“属性”项。



选择“属性”项

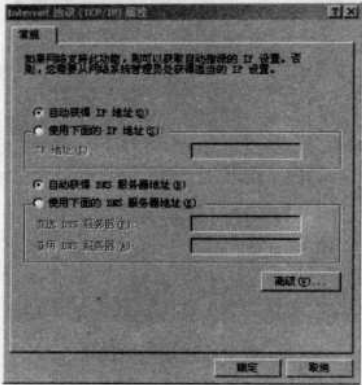
在弹出的“爱博科研究室 属性”窗口的“网络”选项卡设置界面中双击“Internet 协议 (TCP/IP)”项。



双击“Internet协议(TCP/IP)”项

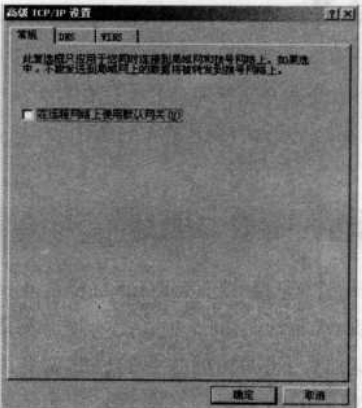
在“Internet 协议 (TCP/IP) 属性”对话框中

点击“高级”按钮继续。



点击“高级”按钮

随即出现的“高级 TCP/IP 设置”对话框中，清空“常规”选项卡设置界面中“在远程网络上使用默认网关”项的选中状态。



“常规”选项卡设置界面

12.3.4 拨入VPN服务器

现在远程用户就可以使用被赋予拨入权限的用户名“administrator”拨入 VPN 服务器了。方法如下：

双击桌面上的“爱博科研究室”图标，在弹出的拨号窗口中的“用户名”和“密码”栏中输入相应的信息后，点击“连接”按钮即可与 VPN 服务器建立连接了。



点击“连接”按钮

连接成功后，远程用户就可以如同服务器所在局域网中的用户那样自由使用局域网内的资源了，如网上邻居、FTP等。



注意

成功建立连接后，客户端在访问服务器端的共享资源时可能会出现长时间的搜索过程。这时可以使用“搜索计算机”功能对指定计算机进行搜索。

12.4 Web接口管理

Web 管理接口 (web management interface) 在 Windows Server 2003 中，是一项非常值得网管使用的功能，这项功能主要的目的就是帮助一些有权限的网络用户（网管）在无法进行本机维护时，提供远程的 Web 管理接口服务，从而实现快捷的简化管理机制。因为这项功能涵盖的面很广，所以下面仅对四项常见的 Web 接口管理服务进行简述。

12.4.1 远程管理打印服务器

打印服务器是 Windows Server 2003 服务器中的一种，是指具有固定的地址，并为网络用户提供服务的节点。下面将从配置和远程管理打印服务器两个方面来讲解相关的应用。

1. 配置打印服务器

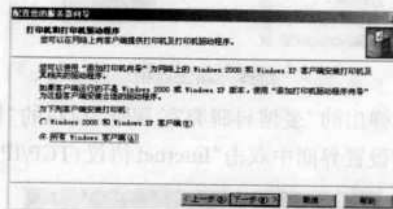
在计算机与打印机完成硬件连接后，依次点

击“开始→设置→控制面板→管理工具”，运行“配置您的服务器向导”。在弹出的“欢迎使用配置您的服务器向导”窗口中点击“添加/删除角色”。在出现“服务器角色”对话框后，选中“打印服务器”项后继续。



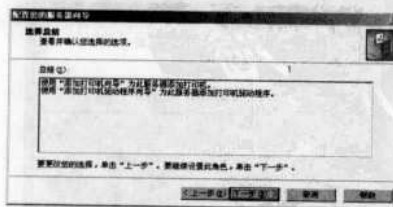
“服务器角色”对话框

在“打印机和打印机驱动程序”对话框中，如果将来使用此打印机的计算机都是 Windows 2000 以上的版本，那么就选中“Windows 2000 和 Windows XP 客户端”项；如果还有计算机是使用 Windows 98 等系统，那么则选择“所有 Windows 客户端”项。这里选择“所有 Windows 客户端”项后继续。



选择“所有Windows 客户端”项

在“选择总结”对话框中点击“下一步”按钮后继续。



点击“下一步”按钮

在出现的“添加打印机向导”中点击“下一步”按钮继续，在“本地或网络打印机”对话框中选择“连接到这台计算机的本地打印机”项后继续。

第十二章 服务器远程管理与维护



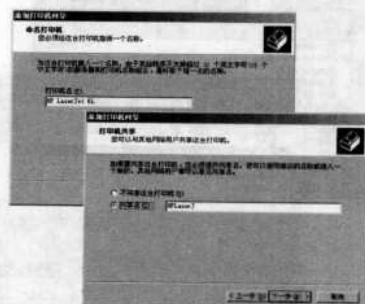
添加打印机向导

在“选择打印机端口”中选择默认状态继续，在“安装打印机软件”对话框中请根据实际情况为打印机安装好驱动（这里是安装了 HP 6L 打印机驱动）。如果在 Windows Server 2003 的内置驱动库中没有当前打印机的驱动，就应点击“从磁盘安装”按钮从打印机随机驱动盘中调用驱动文件进行安装（具体过程略）。



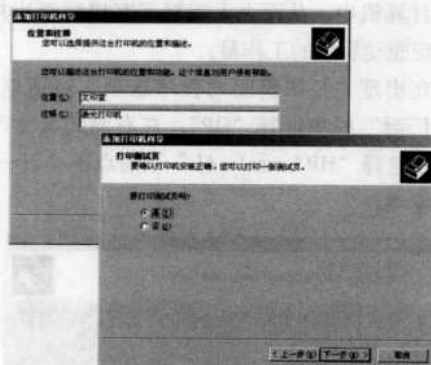
安装向导

在“命名打印机”对话框中选择默认状态继续，在“打印机共享”对话框中选择“共享名”项，并设置好打印机在网络中的共享名后，点击“下一步”按钮继续。



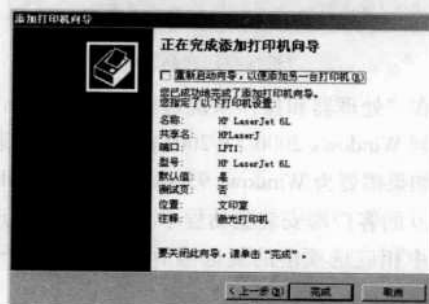
设置共享名

在“位置和注释”对话框中根据实际情况进行相应的信息输入后（输入信息可以有效区分开网络中不同部分的打印机），在“打印测试页”对话框中选择“是”项后继续。



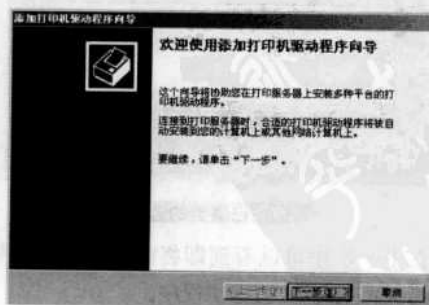
“打印测试页”对话框

在下一步中清空“重新启动向导”项的选中状态后，点击“完成”按钮继续。



点击“完成”按钮

在随后系统自动完成打印机驱动安装后，在随即弹出的“向导”中点击“下一步”按钮继续。

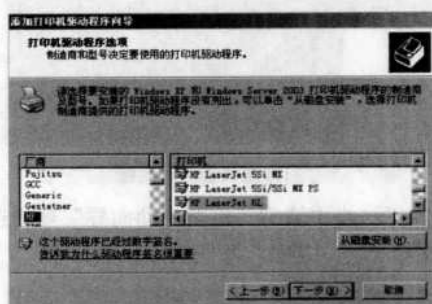


点击“下一步”按钮



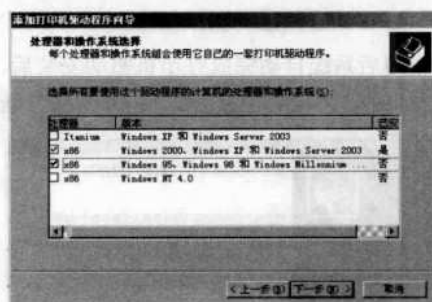
这个向导将帮助用户在打印服务器上安装多种平台（如 Windows XP、Windows 98 等）的打印机驱动。这样，当客户端的用户连接到打印服务器时，合适的打印机驱动将被自动安装到客户端的计算机中，从而大大减轻了客户端查找并安装相应驱动程序的工作量。

在出现“打印机驱动程序选项”对话框后，在“厂商”栏中选择“HP”，在右侧的具体产品列表中选择“HP LaserJet 6L”项后点击“下一步”按钮继续。



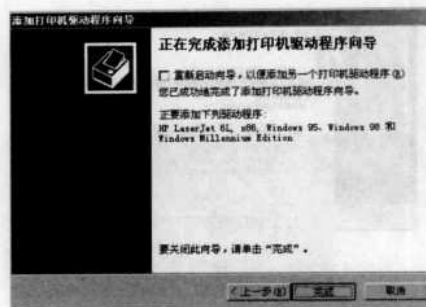
选择打印产品

在“处理器和操作系统选择”对话框中，可以看到 Windows 2000/XP/2003 的驱动已经安装好了。如果需要为 Windows 95/98/ME 或是 Windows NT 4.0 的客户端安装驱动程序的话，需要勾选对话框中相应选项前的复选框后，点击“下一步”按钮继续。



勾选自己需要的选项

在下一步中可以看到即将添加当前打印机的 Windows 95/98/ME 的驱动程序。



完成操作

2. Web管理

在 Windows Server 2003 中，如果在配置好打印服务器的同时也安装了 IIS，则有权限的网络用户就可以通过 IE 等浏览器来管理打印服务器，域中的用户也可以通过浏览器来安装打印机、管理自己打印的文档等。这种方便的管理模式就是“打印机服务器 Web 接口管理方式”。实现的过程如下：

因为在 Windows Server 2003 中，默认状态下是不安装 IIS 6.0 的，所以需要先安装 IIS 6.0 和相关的远程管理组件，方法是：

依次点击“开始→控制面板→添加/删除程序”，在打开“添加或删除程序”窗口中点击窗口左侧导航栏中的“添加/删除 Windows 组件”按钮，接着在弹出的“Windows 组件向导”窗口中选择“应用程序服务器”。双击“应用程序服务器”后，在弹出的窗口中点击勾选“Internet 信息服务 (IIS)”。因为要设置打印机服务器可以使用 Web 接口方式的管理，所以还需要接着点击“详细信息”按钮。



点击“详细信息”按钮

第十二章 服务器远程管理与维护

只有在弹出的窗口中点击勾选“Internet 打印”选项后，这样才能实现 Web 打印及管理打印机。

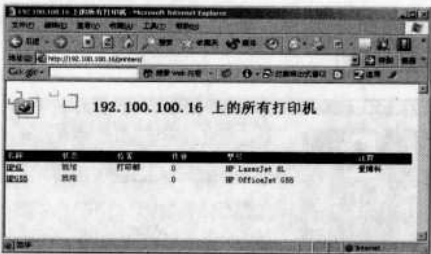


勾选“Internet打印”选项

接着连续两次点击“确定”按钮返回到安装向导后点击“下一步”按钮，根据系统提示放入 Windows Server 2003 光盘，开始安装上述设置添加的组件。在组件安装完毕后，就可以在网络中的任一台计算机上（以局域网为例）输入以下格式的网址进入打印机服务器的 Web 接口管理页面了：

http:// 打印服务器名称 /printers/ 如：http://192.100.100.16/printers/

在输入网址并回车后，可以看到当前网页中已经列出了这台服务器上的所有打印机及状态。

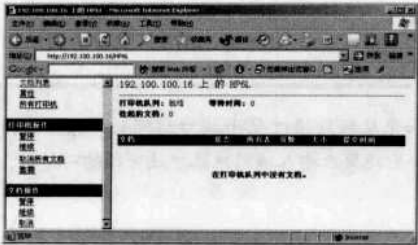


服务器上所有打印机及状态

注意

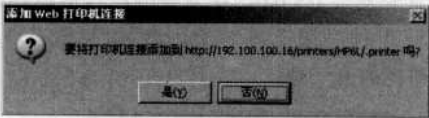
根据打印服务器的安全设置不同，有可能需要输入管理员用户名和密码才能出现上述页面。

当然此外也可以直接输入“打印服务器名称 / 打印机共享名”的网址直接进入选中的那台打印机管理页面，如“http://192.100.100.16/HP6L”。



打印机管理页面

如果想在客户端安装打印服务器中的打印机的话，则可以通过 Web 接口来完成打印机的驱动安装。方法是：点击上图左侧的“连接”，打开“添加打印机连接”提示框。



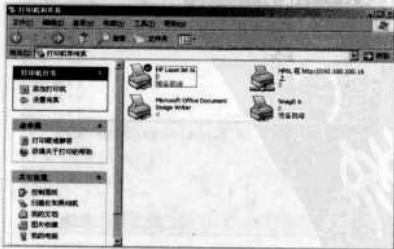
“添加打印机连接”提示框

接着在下一步的“配置 Internet 端口”窗口中根据实际情况进行选择后，点击“确定”按钮继续。



配置 Internet 端口

在安装完成后，可以在客户端的打印机文件夹中看到已安装成功的打印机名称。接下来就可以使用刚装好的打印机打印文档了。



装好的打印机打印文档



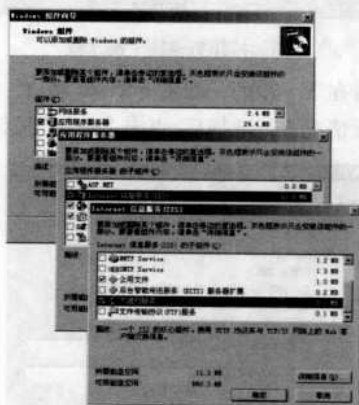
注意

如果从域外通过 Web 接口访问打印服务器，连接时就会出现要求输入域用户账户及密码的对话框。

12.4.2 终端服务器的Web接口管理

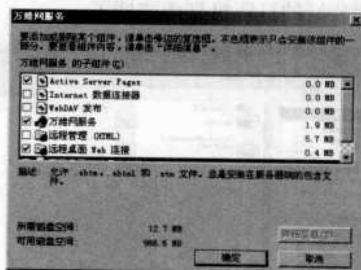
因终端服务器的配置方法在本章 12.2 一节中已经讲述过了，所以在本小节中将直接讲解终端服务器的高级管理方法——终端服务器的 Web 接口管理功能。

首先安装 IIS 6.0。在安装的过程中请逐级选中“应用程序服务器→Internet 信息服务 (IIS)→万维网服务”项。



选择服务

接着双击“万维网服务”，在弹出的窗口中点击勾选“远程桌面 Web 连接”功能后，连续按三次“确定”按钮返回到安装向导，并点击“下一步”按钮开始安装选中的组件。



安装组件

安装“远程桌面 Web 连接”组件后，就可以在远程计算机中在 IE 的地址栏中输入如下格式访问终端服务器了：

http:// 服务器 IP 地址或名称 /tsweb/，

如，http://192.100.100.16/tsweb/。

按回车键后，将会在当前网页中显示出“远程桌面 Web 连接”页面。



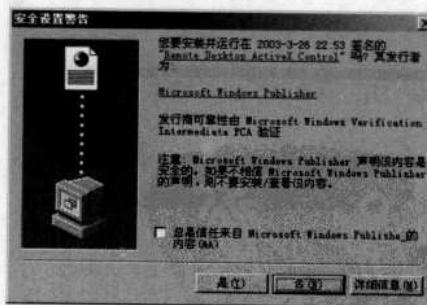
远程桌面Web连接



注意

根据服务器的安全设置不同，有可能需要输入管理员用户名和密码才能出现上述页面。

在随即弹出的“安全设置警告”提示框中点击“是”按钮。

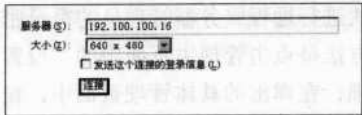


安全设置警告

稍待片刻后，在“远程桌面 Web 连接”页面中输入服务器的 IP 地址以及设置好显示的分辨率大小。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十二章 服务器远程管理与维护



显示的分辨率大小

接着点击“连接”按钮就可以登录到终端服务器的登录界面了。



终端服务器的登录界面

此时只需在登录对话框的“用户名”和“密码”两项右侧的文本框中，输入正确的用户名和密码就可以登录到该服务器的桌面环境了。

12.4.3 流媒体服务器的Web管理接口

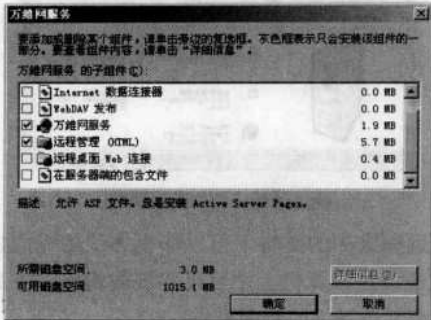
随着宽带网络的普及，在线实时收看视频也成了一种时尚，如果你也想架设这样一台既可以进行网络广播，又可以进行视频点播的流媒体服务器，供网友们进行实时视频交流。那么请参看第十章“10.4 用 IIS6.0 搭建流媒体服务器”一节。

12.4.4 远程维护Web接口

远程维护功能是一项非常重要的网络维护与管理功能，它可以帮助网络管理员通过 Web 接口来完成服务器的多个具体服务项目的管理维护操作，也就是远程进入 IIS 6.0 Web 接口管理页面。

依次点击“开始→设置→控制面板→添加/删除 Windows 程序”菜单项，点击窗口左边的“添加/删除 Windows 组件”按钮，在稍弹出的“Windows 组件向导”窗口中逐层依次选择“应用

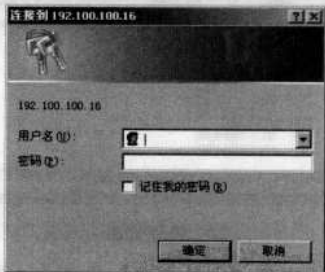
程序服务器→Internet 信息服务 (IIS)→万维网服务”项，点击勾选其下的“远程管理 (HTML)”一项，并点击“确定”按钮进行该组件的安装。



组件的安装

完成上述操作后，就可以在局域网中输入“https:// 服务器名称或 IP 地址 :8098”这样的格式（在远程计算机中只能输入“https:// 服务器 IP 地址 :8098”），来访问 Windows Server 2003 的 IIS 6.0 的 Web 接口管理页面了。

但根据服务器的安全设置不同，有可能需要输入管理员用户名和密码才能出现上述页面。也就是说，输入的用户名必须具有相应的管理权限，否则登录之后无法进行维护操作。



输入用户名和密码

以管理员身份登录系统后，在登录的管理页面中显然可以看出在这里可以进行 Web 等各种服务器的具体设置。如，能够查看或配置服务器的运行日志文件、当前运行状态、网站 IP 地址、DNS 后缀、域。此外还能够创建、编辑、删除服务器上的用户和组名单，甚至可以远程重新启动服务器、关闭服务器或者是通过计划任务关闭计算机。



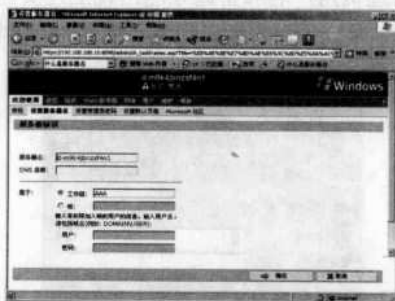
通过计划任务关闭计算机

远程维护的支持下可以非常方便的完成以前必须亲自在计算机上才可以实现的操作。下面就来讲解几个基本的管理操作：

1. 设置服务器名

设置服务器名可以使网络中称谓管理更加合理，资源的寻找更加方便，例如需要将当前服务器加入到一个域中，那么服务器名就往往需要更改。在 Web 管理模式中，修改服务器名是件很容易的事情。方法为：

点击“设置服务器名”项，弹出具体设置界面。



具体设置界面

在上图中将“服务器名”右侧文本框中的名称删除，然后重新输入所需的名称即可完成服务器名的设置、修改了。在此设置界面中，如果需要将当前服务器由“工作组”管理模式改为加入到“域”管理模式，只需点击“域”选项前的单选框，并输入设置相应的域名即可。修改完成后，请记得需要点击管理页面右下角的“确定”按钮来确认操作的执行。

2. 设置管理员密码

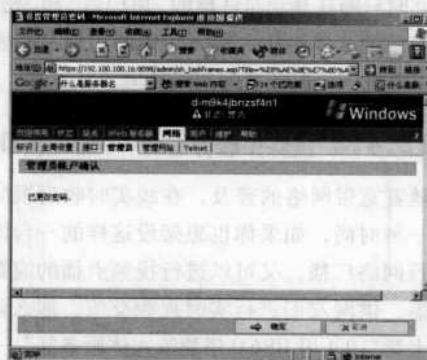
这个操作比较容易理解，意思就是可以通过

Web 方式进行远程服务器管理员的登录密码修改操作。方法是点击管理主页面中的“设置管理员密码”项，在弹出的具体管理页面中，输入当前登录的密码，然后再重复两次输入需要更改的密码，并点击“确定”按钮即可完成管理员密码的修改。



完成管理员密码的修改

要注意的是，在修改管理员密码操作完成后，当再次通过本机登录或 Web 接口登录服务器时，就需要使用更改后的密码才能登录了。



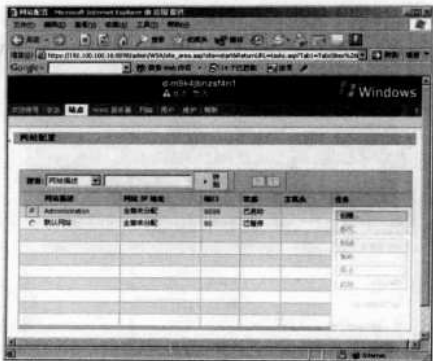
用更改后的密码登录

3. 创建FTP服务

通过 Web 接口管理服务器，除了可以进行一般性的操作外，只要权限允许，还可以创建、删除、修改站点。以创建一个 FTP 服务为例，方法如下：

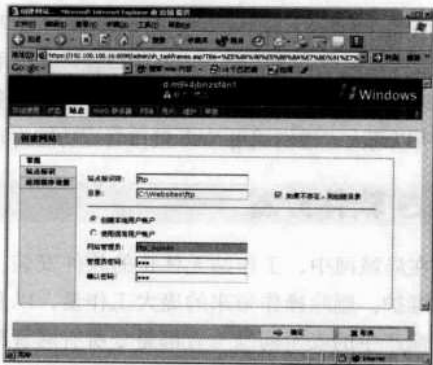
点击 Web 管理页面中上方的“站点”标签，转换到站点管理页面。

第十二章 服务器远程管理与维护



站点管理页面

点击页面右侧部分“任务”列表中的“创建”按钮，弹出“创建网站”页面。



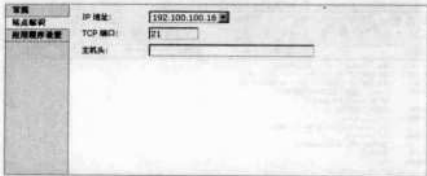
弹出“创建网站”页面

在“站点标识符”右侧的文本框中输入准备创建的服务名，如FTP。接着按键盘上的“TAB”键切换到下一项，此时目录中将自动出现默认创建的目录；下面的“网站管理员”项的文本框中也将自动出现该服务所对应的默认管理员名称，如“FTP_Admin”。接着再在“管理员密码”和“确认密码”两项右侧的密码框中输入相同的密码。

此时请不要急着点击下方的“确定”按钮执行当前的操作，因为此时创建的站点服务端口并不是FTP服务默认的21端口，而是与默认网站相同的80端口，如果此时点击“确定”按钮的话，那么就会造成端口资源冲突的现象了。

正确的做法是，点击上图中左侧的“站点标识”项，在进入相应的管理页面后，将“TCP 端口”项右侧文本框中的数字“80”删除，输入数字“21”

(端口21为默认的FTP服务端口)。接着点击“IP地址”项右侧的下向箭头，在下拉菜单中选中需指定的IP地址，如192.100.100.16。



需指定的IP地址

设置完毕后，此时才可以点击“确定”按钮执行当前的操作。稍后在返回到的“网站配置”管理页面中可以看到刚刚创建的名为“FTP”服务。



创建服务

从上图中可以看出，创建的服务“状态”为“已停止”，这说明当前服务创建成功了，但还没有被激活，所以此时应点击右侧“任务”列表中的“启动”按钮，将其激活。

如果“状态”中没有在点击“启动”按钮后，即时出现“已启动”的字样，请不要反复尝试，因为此时如果使用Cuteftp这类的FTP软件尝试登录的话，就会发现登录将会立即成功，也就是说服务实际上已经成功了。下图为在Cuteftp中需要设置的信息。



Cuteftp中需要设置的信息

登录成功的界面中，可以看到创建的FTP服



务已经可以使用自动创建的 FTP 管理账户和我们设置的密码登录了。而且系统还在自动创建的目录中又创建了一个“新建文件夹”。



创建“新建文件夹”

在登录成功后，就可以进行文件的上传、下载、更名、删除等操作了。

4. 更改Web服务的目录

这个操作需要使用 FTP 服务和更改 Web 服务目录两个操作来组合完成，假设现在需要更改 Web 服务的目录，那么下述方法如下：

通过使用上面讲解的开启 FTP 服务方法开启 FTP 服务，如果 FTP 在服务器已经开启了，那么请直接使用 Cuteftp 客户端程序登录到服务器，并且将 Web 服务器中的所有文件复制到指定的目录中，如将“c:\inetpub”目录中的文件复制到“D:\www”目录中。具体操作略。

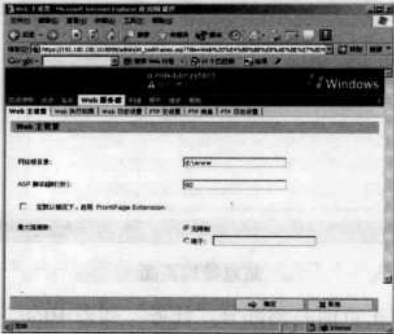
接着在 Web 管理页面中依次点击工具栏中的“Web 服务器”项，在随即弹出的“Web 服务器”页面中点击“Web 主设置”项。



点击“Web主设置”项

在稍后打开的“Web 主设置”页面中，将

“网站根目录”对话框中输入目的目录名即可，如“D:\www”。最后点击“确定”按钮即可完成 Web 服务器根目录的重新设置操作。



根目录的重新设置

虽然 Windows Server 2003 的 Web 接口管理功能很强大，但要强调的是，Web 接口管理会因为用户的管理是否妥当，而有可能出现不同等级的安全隐患，所以请大家谨慎使用 Web 接口管理功能为宜！

12.5 软件分发

在局域网中，工作站无休止的软件安装、升级、维护、删除操作带来的庞大工作量，以及因此可能产生的安全问题一直都是令所有网管都头疼的事情！这个时候，支持远程管理的“软件分发”功能就可以大显身手了。

简单地说，软件分发就是将软件分布发送到指定工作站的功能。以往，很多管理员都是采用了共享的方法，但共享所能引起的安全隐患往往会成为网管们心中永远的痛！此时，如果你尝试使用软件分发功能的话，那么你会惊喜地发现工作站的软件安装将会变得轻松自如且安全无忧！

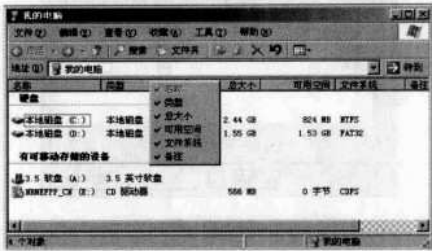
假设现在一位网管要将 shyzhong.com 域中的“Windows Server 2003 管理工具包”程序“Adminpak.msi”分发到所有的工作站上，那么则应进行如下设置：

12.5.1 设置共享目录

为了最大程度地进行访问权限的管理，首先应在使用 NTFS 文件系统的分区中新建一个目录。在 Windows Server 2003 中有很多方法可以看出

第十二章 服务器远程管理与维护

当前分区是否使用了 NTFS 文件系统，其中最简单的莫过于在“我的电脑”窗口中右键点击“快捷功能工具栏”后，在弹出的菜单中选择“文件系统”项后，在分区右侧就可以看到相应文件系统的方法了。



选择“文件系统”项后

从上图中可以看出 C 盘使用的是 NTFS 文件系统。所以现在就可以在 C 盘中新建一个名为“Tools\$”的目录了。然后将“Adminpak.msi”程序从 Windows Server 2003 安装光盘的“i386 目录”中复制到 C 盘的“tools\$”目录中。



复制到C盘的“tools\$”目录

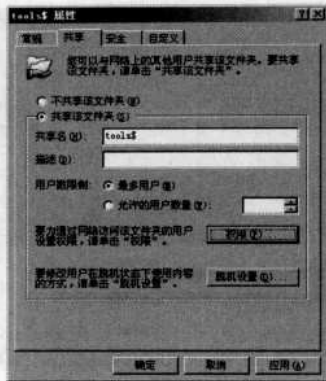


注意

准备用于共享的目录名，如果带有“\$”符号，则网络中不能看到这个目录，但可以通过输入路径的方法来访问到它；如果不带有“\$”符号，则网络中可以看到它。在软件分发操作中，只有让用户在网络中不能直接看到共享目录，才能把管理和控制权牢牢地把握在网管手中。

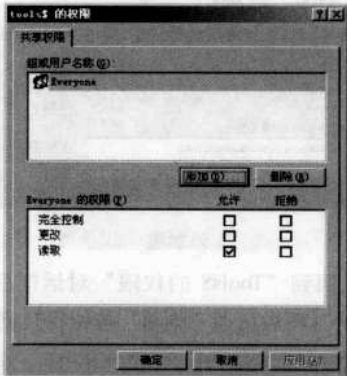
接着在 C 盘中右键选中“Tools\$”目录并单击，在弹出的快捷菜单中选择“共享与安全”项，在弹出的“Tools\$ 属性”对话框的“共享”选项

卡设置界面中，点击勾选“共享该文件夹”项后，点击下方的“权限”按钮。



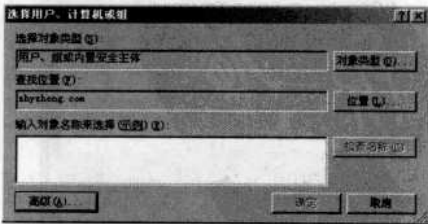
“权限”按钮

在弹出的“Tools\$ 的权限”对话框中，点击“添加”按钮。



点击“添加”按钮

在“选择用户、计算机或组”窗口中点击“高级”按钮。



点击“高级”按钮

在随之切换的窗口中点击“立即查找”按钮，将当前系统中的用户、计算机等资源查找出来，在按住 Ctrl 键的同时，使用鼠标单击选择其中的

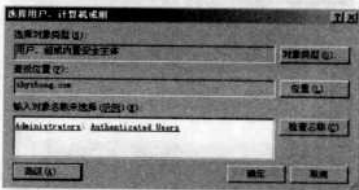


“Administrator”组和“Authenticated Users”组后，点击“确定”按钮。



选择组

在返回到标准模式的“选择用户、计算机或组”窗口后，可以看到选中的两个组均已添加，此时请点击“确定”按钮。



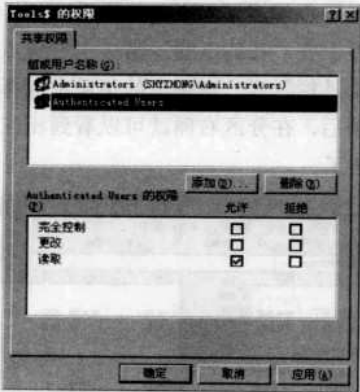
添加组

在返回到“Tools\$ 的权限”对话框后，选中“Everyone”项后点击“删除”按钮将其删除。



权限设置

接着分别选中“Authenticated Users”组，将其共享权限设置为“读取”、选中“Administrators”组后，将其权限设置为“完全控制”。



完全控制



注意

分发的软件必须是 MSI 封装文件，如果想将非 MSI 格式的文件封装成 MSI 文件，可以使用 InstallShield 等工具来完成这个转换操作。当然，也可以使用 ZAP 文件来分发非 MSI 格式的文件。

12.5.2 设置组策略

以域管理员身份登录 DC（即域控制器），然后依次点击“开始→程序→管理工具→Active Directory 用户和计算机”菜单项，在弹出的窗口中选中并右键单击“shyzhong.com”，在弹出的快捷菜单中选择“属性”。



组策略编辑栏

接着在打开的“属性”窗口中点击“新建”按钮，并将新建的组策略对象命名为“Software”。

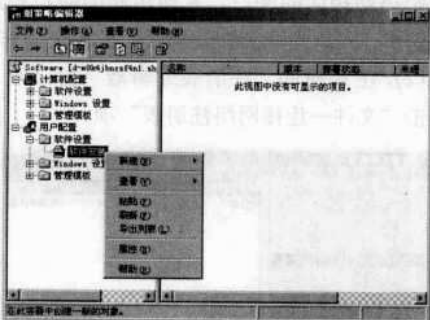
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十二章 服务器远程管理与维护



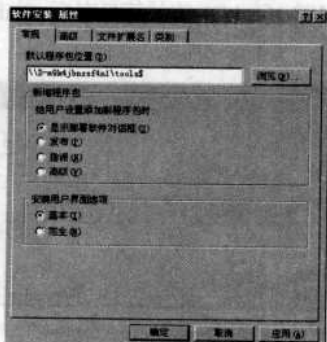
点击“新建”按钮

接着选中 Software 并单击下方的“编辑”按钮，在打开的“组策略编辑器”窗口中依次点击“用户配置→软件设置→软件安装”项。接着右键单击“软件安装”项，并在弹出的快捷菜单中选择“属性”。



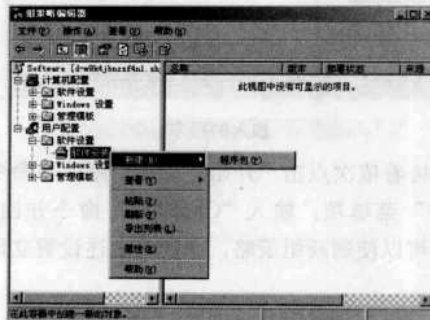
选择“属性”

在弹出的“软件安装 属性”对话框中手工输入“\\计算机名\共享文件名”（如“\\D-m9k4jbnzsf4n1\tools\$”），然后点击选中“显示部署软件对话框”和“基本”两项。



设置“软件安装”属性

点击“确定”按钮返回后，右键选中并点击“软件安装”项，在弹出的快捷菜单中依次选择“新建→程序包”项。



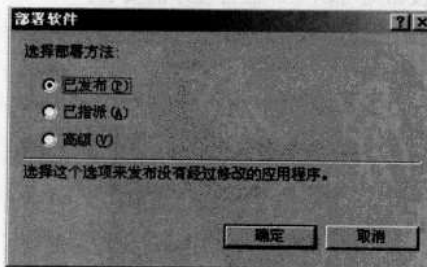
新建程序包

在随后弹出的“打开”对话框中，选中 tools\$ 目录下的“Adminpak.msi”文件后，单击“打开”按钮。



打开文件

在随后弹出的对话框中点击选中“已发布”项后，点击“确定”按钮。稍后关闭组策略对话框。



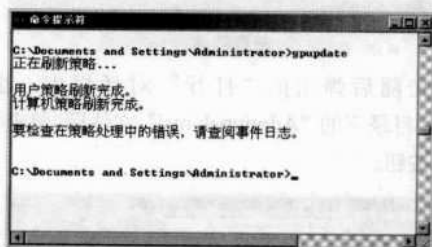
关闭组策略对话框

稍后在组策略窗口的“软件安装”项右侧窗口可以看见刚刚加入的程序包。



加入的程序

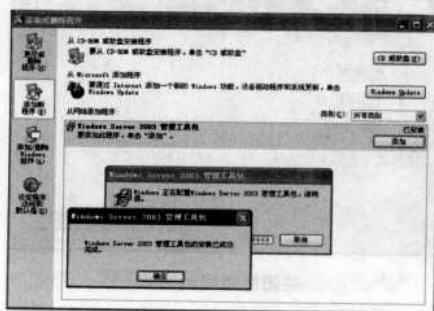
接着依次点击“开始→程序→附件→命令提示符”菜单项，输入“Gpupdate”命令并回车，这样可以使刷新组策略，以便使上述设置立即生效。



刷新组策略

12.5.3 在工作站中安装软件

经过上述的设置后，软件就会被分发到 shyzhong.com 域中的所有工作站上了。在工作站中（以 Windows XP 为例），当用户登录域后，只需点击“添加/删除程序”窗口中的“添加新程序”按钮，就会立即在“从网络添加程序”列表中列出 DC 中分发的“Adminpak.msi”程序了。点击“添加”按钮则可以立即进行程序的安装。



进行程序的安装

12.6 远程管理注册表与组策略

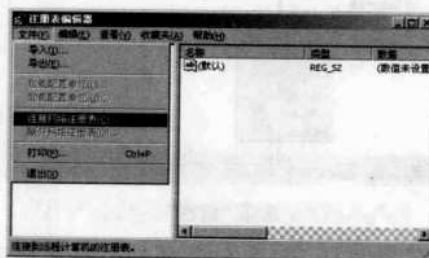
由于注册表是系统的核心数据库，所以对它进行远程管理将会具有积极的意义。此外，为了使远程管理变得更加方便，我们可以使用远程管理组策略的方法。

12.6.1 远程编辑注册表

远程编辑注册表是一项常规操作，它可以让熟悉注册表维护的用户对远程用户出现问题的注册表进行维护。要进行此项操作，可以使用 Reg 命令等多种方法。这里介绍在“注册表编辑器”中实现远程编辑的方法。以 A 机连接到 B 机为例，具体过程是：

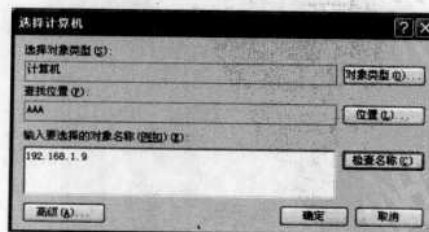
(1) 在 A 机中新建一个与 B 机当前登录账户名和密码均相同的账户，并使用新的账户登录 A 机。这样，可以避免连接注册表时的验证操作；

(2) 在 A 机的“注册表编辑器”窗口中，依次单击“文件→连接网络注册表”项；



注册表编辑器

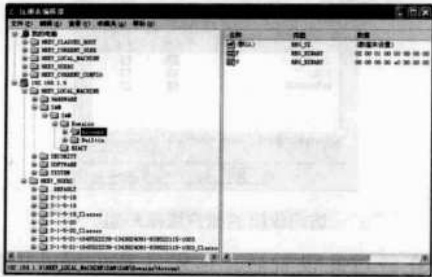
(3) 在弹出的“选择计算机”窗口中，在“输入要选择的对象名称”栏中输入远程计算机的 IP 地址（如 192.168.1.9）或计算机名后，单击“确定”按钮；



输入远程计算机的IP地址

第十二章 服务器远程管理与维护

(4) 随即，就可以在“注册表编辑器”窗口中的左侧，看到远程计算机的 IP 地址，其下的内容便是远程计算机的可以编辑的注册表内容范围，



注册表内容范围

(5) 当完成对远程注册表的编辑操作后，依次单击“文件→断开网络注册表”菜单，可以中断对远程注册表的连接。



中断对远程注册表的连接

在远程注册表连接完成后，远程注册表默认允许对 HKEY_LOCAL_MACHINE 和 HKEY_USERS 子树进行编辑。如果希望精确定制这两根子树中的可以访问的范围，需要在组策略中进行如下操作：

- (1) 在“运行”栏使用命令“Gpedit.msc”打开“组策略”窗口；
- (2) 依次展开到如下分支：
计算机配置\Windows 设置\安全设置\本地策略\安全选项
- (3) 双击右侧窗格中的“网络访问：可远程访问的注册表路径”项，在弹出的如图所示属性窗口中可以看到默认允许的子树中的范围有哪些，在这里可以添加和删减具体的子项路径。



添加和删减具体的子项路径

由于这里的定义需要在注册表中做出相应的配合，所以还需要执行如下操作：

- (1) 在“注册表编辑器”窗口中，依次展开到如下分支：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

- (2) 在 winreg 子项的 AllowedPaths 项中，双击右侧窗格中的“Machine”值，在弹出的属性窗口中可以看到组策略中“网络访问：可远程访问的注册表路径”的策略设置在这里有着相同的值。实际上，“网络访问：可远程访问的注册表路径”策略的设置目的，就是为了供“Machine”值调用。

注意

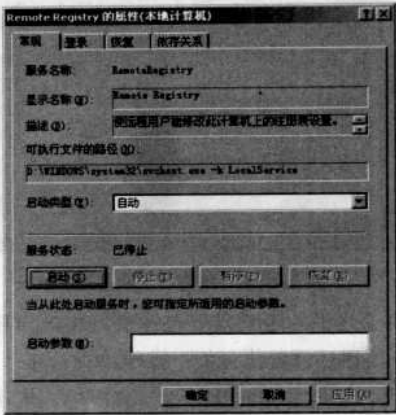
Windows XP Professional 中，默认情况下只有管理员组和备份操作员组的成员才有权通过网络访问注册表。管理员具有完全控制访问权，备份操作员具有读访问权。而在 Windows XP Home Edition 中，默认情况下只有管理员组的成员才可以通过网络访问注册表。管理员具有完全控制访问权。

在 Windows XP 中，除了组策略中有关于远程访问注册表的值外，在系统“服务”中也有一项专门针对远程注册表访问的服务，此服务可以控制远程访问注册表这个环境是否被提供。

- (1) 在“运行”栏中使用命令“Services.msc”打开“服务”窗口；
- (2) 双击“Remote Registry”服务，在弹出的如图所示属性窗口中，如果设置此服务为“停止”



状态，那么只有此计算机上的用户才能修改注册表。默认状态下，此服务处于启动状态。

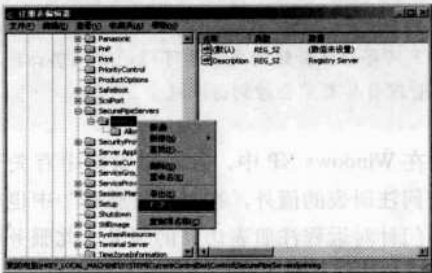


修改注册表

除了可以通过服务来决定远程注册表是否可以访问外，还可以通过如下方法指定只有哪些账户或组能够远程访问注册表的 HKEY_LOCAL_MACHINE 子树。

(1) 在“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg”子项中，新建一个名为“Description”的 REG_SZ 的值，并设置其属性内容为“Registry Server”；

(2) 选中“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers”子项中的“winreg”项并单击右键，在弹出的快捷菜单中选择“权限”；



选择“权限”

(3) 在弹出的如图所示窗口中，指定授予各种访问权限的账户或账户组即可。



访问权限的账户或账户组

在经过此设置后，远程计算机可以连接到 HKEY_LOCAL_MACHINE 和 HKEY_USERS 子树，但是，其中 HKEY_LOCAL_MACHINE 会受到访问权限（如不能打开子项列表，等等）的控制，而 HKEY_USERS 则可以任意打开。

如果要绕过 Winreg 子项给出的访问权限限制，需要执行如下操作：

(1) 在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg 子项下新建一个名为“AllowedPaths”的项；

(2) 选中“AllowedPaths”项后，在右侧窗格中新建名为“Machine”的 REG_MULTI_SZ 值。

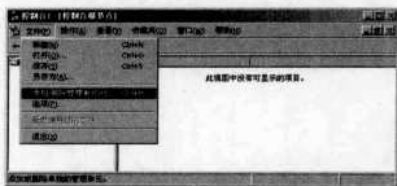
(3) 双击“Machine”值，在其中添加希望绕过访问限制的那些注册表项即可。前面已经说过，这个值的属性内容实际上与“组策略”的“计算机配置\Windows 设置\安全设置\本地策略\安全选项”分支中，“网络访问：可远程访问的注册表路径”项的属性内容是相同的。因此，设置“Machine”值和“网络访问：可远程访问的注册表路径”项都是可以的。

12.6.2 远程管理组策略

以工作组环境为例，要对其他计算机的组策略进行远程管理，使用 Gpedit.msc 是无法实现的。我们必须在控制台添加一个新的组策略管理单元来实现这个远程管理。具体的实现过程是：

(1) 在“运行”栏中使用命令“MMC”打开“控制台 1”窗口后，依次单击“文件→添加 / 删除管理单元”菜单；

第十二章 服务器远程管理与维护



“控制台1”窗口

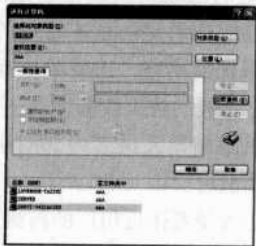
(2) 弹出的“添加/删除管理单元”窗口中，可以看到有“独立”和“扩展”两种类型的管理单元。独立管理单元是最常见的管理单元，它通常只由一个功能相对独立的管理工具组成。扩展管理单元则可以看成是一个管理单元集中的附属单元，换句话说，就是当一个管理单元中包含多个功能对相分离的管理工具集合时，其中的每个管理工具都可以看成是扩展管理单元。

(3) 因为组策略对象编辑器属于“独立”类型，所以要在“独立”选项卡界面单击下方的“添加”按钮。在弹出的窗口的列表中选择“组策略对象编辑器”项后单击“添加”按钮；

(4) 自动弹出的向导窗口中，默认是添加基于本地的组策略对象编辑器。

(5) 如果希望添加基于其他计算机的组策略对象编辑器，则需要单击“浏览”按钮打开窗口，在这里勾选“另一台计算机”项后，在下方的地址栏中输入远程计算机名或 IP 地址后，单击“确定”按钮即可。如果记不得远程计算机的 IP 地址或计算机名，则需要单击“浏览”按钮。

(6) 单击“浏览”按钮，在弹出的“选择计算机”窗口中，单击“高级”按钮打开扩展界面后，单击“立即查找”按钮找到要添加的远程计算机；



添加的远程计算机

(7) 单击“确定”按钮返回“选择计算机”窗口后，再单击“确定”按钮关闭此窗口；

(8) 接着，在弹出窗口中需要输入远程计算机的管理员账户名与密码。如果不想出现这个窗口，只需在本地计算机中创建一个远程计算机中的管理员账户（具有相同的密码），并使用这个账户登录本地计算机即可。如果没有出现这个窗口，请检查远程计算机的“本地连接”或“Windows 防火墙”中是否勾选启用了“文件和打印机”共享服务。如果出现这个窗口，但只能使用 Guest 账户（用户名呈不可更改的灰色），则需要远程计算机中的“文件夹选项”窗口中取消“使用简单文件共享（推荐）”项的选中状态。

(9) 返回后单击“完成”按钮开始连接远程计算机的组策略对象编辑器工具。此时，使用的账户必须具有管理员权限，否则将无权限访问远程计算机的组策略对象编辑器工具。

(10) 连接上远程计算机后，会自动进入如图所示的窗口，在列表中可以看到针对远程计算机的组策略对象编辑器已经创建成功了。



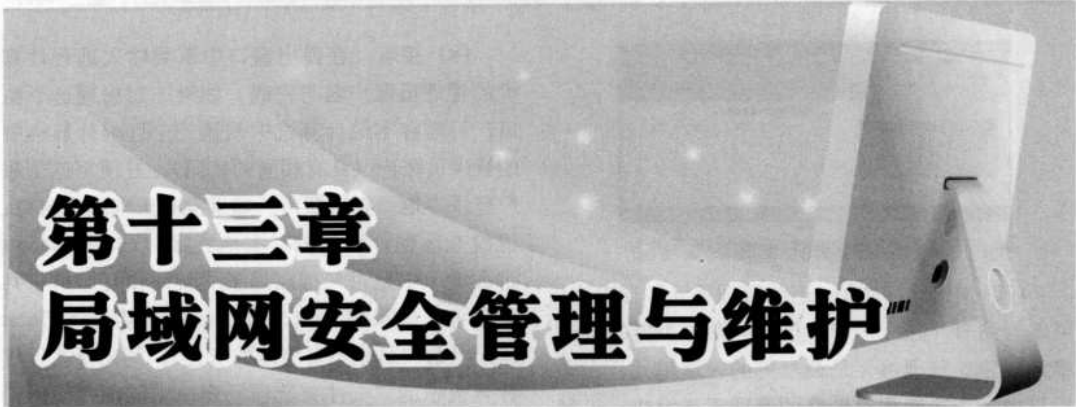
创建编辑对象

(11) 单击“确定”按钮返回到如图所示的窗口后，可以看到“控制台根节点”列表中已经有了远程计算机的组策略树。



远程计算机的组策略树

此时，在本地进行的远程组策略设置，将会在远程计算机的组策略窗口中同时自动进行，从而实现了远程计算机的组策略管理。



随着计算机网络技术的突飞猛进，网络安全的问题已经日益突出地摆在各类用户的面前。有关资料表明，目前在互联网上大约有将近 20% 以上的用户曾经遭受过黑客的困扰。尽管黑客如此猖獗，但网络安全问题至今仍没有能够引起足够的重视，更多的用户认为网络安全问题离自己尚远。很多用户一直以为网络安全问题好像是有人故意在喊“狼来了”，可是当狼真的来了的时候，你做好准备了吗？构建安全网络，保证网络安全，这就是本章内容所要阐释的。

13.1 配置防火墙保障局域网安全

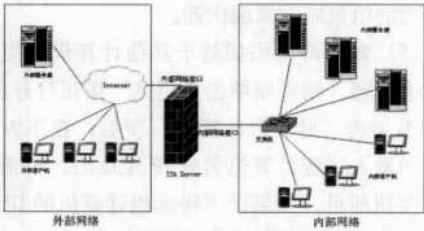
如果说大约有 40% 以上的用户特别是企业级用户没有安装网络防火墙，也许读者会对这个数字感到不以为然。也难怪，一个干巴巴的数字能代表什么呢？而事实却是，几乎所有的迹象都在向大家证明一个事实，大多数的黑客入侵事件都是由于未能正确安装和配置防火墙而引发的。于是用户不得不正视防火墙对于构建安全网络的重要作用。

13.1.1 防火墙简述

防火墙的本义原是指古代人们房屋之间修建的那道墙，这道墙可以防止火灾发生的时候蔓延到别的房屋。而这里所说的防火墙当然不是指物理上的防火墙，而是指隔离在本地网络与外界网络之间的一道防御系统，是这一类防范措施总称。

应该说，在互联网上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域（即 Internet 或有一定风险的网络）与安全区域（局域网）的连接，同时不会妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信量，从而完成看

似不可能的任务，即仅让安全、核准了的信息进入，同时又抵制对企业构成威胁的数据。



随着安全性问题上的失误和缺陷越来越普遍，对网络的入侵不仅来自高超的攻击手段，也有可能来自配置上的低级错误或不合适的口令选择。因此，防火墙的作用是防止不希望的、未授权的通信进出被保护的网路，迫使单位强化自己的网络安全政策。一般的防火墙都可以达到以下目的：

- (1) 可以限制他人进入内部网络，过滤掉不安全服务和非法用户；
- (2) 防止入侵者接近用户的防御设施；
- (3) 限定用户访问特殊站点；
- (4) 为监视 Internet 安全提供方便。

由于防火墙假设了网络边界和服务，因此更适合于相对独立的网络，譬如 Intranet 等种类相对

第十三章 局域网安全管理与维护



集中的网络。防火墙正在成为控制对网络系统访问的非常流行的方法之一，而事实上在 Internet 上的 Web 站点中，超过 1/3 的 Web 站点都是由某种形式的防火墙加以保护的。这是一种对黑客防范最严、安全性较强的方式。因此，任何关键性的服务器都建议放在防火墙之后。

13.1.2 用ISA Server部署企业级防火墙

网络安全永远是大家最关心的问题。微软总部商业安全与技术部产品经理曾经总结说 70% 以上的攻击是针对网络应用层的。传统防火墙仅对数据包中的 IP 数据头或者 TCP 数据头进行检查，对紧随其后的应用层不做任何处理，所以无法抵御来自应用层的攻击。

作为著名的路由级网络防火墙，ISA Server (Microsoft Internet Security and Acceleration Server) 引入了深度防护的概念。即通过内置多个常用协议过滤器，对应用层进行多层的过滤，从而实现对数据内容的惊喜控制、命令和消息过滤、接口拦截、只读支持、媒体属性过滤、DNS 入侵检测及 POP3 入侵检测等安全防范功能。与旧版本的 ISA Server 相比，新版本的 ISA Server 不仅在功能方面更加强大，尤其在人性化设计方面明显进步。下面以 ISA Server 为例探讨一下如何部署企业级的防火墙，以加强企业网络的安全。

1. 系统及网络需求

安装 ISA Server 的服务器需要满足以下软硬件要求：

CPU：PIII 500MHz 及以上主频的 CPU，推荐使用主频在 1GHz 以上的 CPU。ISA Server 最多可以支持四颗 CPU。

内存：应当配置 256MB 以上容量的内存，推荐容量为 512MB。尽管在实际操作中配置 64MB 的内存也可以运行 ISA Server，但是性能可想而知会很差。

硬盘：ISA Server 的安装分区至少应该有 150MB 空闲空间，不过这个空间要求并不包含缓存使用的磁盘空间。推荐安装分区空闲空间容量大于 1GB。

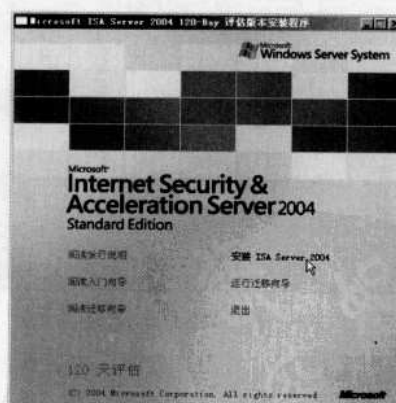
网卡：必须为连接到 ISA Server 服务器的每个网络单独准备一个网卡，至少需要一个网卡。但是在单网卡计算机上安装的 ISA Server 服务器通常是对外发布的服务器提供一层额外的应用程序筛选保护或者缓存来自 Internet 的内容使用。

操作系统：ISA Server 可以运行在 Windows Server 2003 或 Windows 2000 Server 系统平台上，不过强烈推荐将 ISA Server 安装在 Windows Server 2003 系统中。如果在运行 Windows 2000 Server 的服务器上安装 ISA Server，则必须安装 Windows 2000 Service Pack 4 和最新的 KB821887 更新程序，并且需要将 Internet Explorer 升级到 6.0 以上版本。

网络环境：安装 ISA Server 服务器以前应当确保网络能够正常工作，最大限度地排除一些未知因素的干扰。

2. 安装ISA Server服务器

尽管 ISA Server 融入了众多人性化设计，使用户在配置和管理过程中非常便捷，但这种便捷来自于正确的安装设置。在满足上述所列出的系统和网络要求以后，ISA Server 的安装依然不能小觑。本例以在非 AD 域网络环境中安装 ISA Server 简体中文标准版为例，简述其安装过程。



ISA Server安装界面

STEP 1 打开 ISA Server 标准版安装光盘，运行“ISAAutorun.exe”程序，进入安装界面，并单击“安装 ISA Server”按钮。

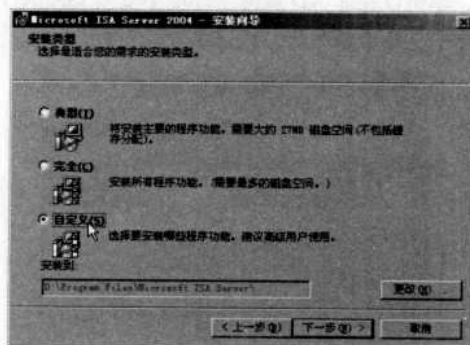


STEP 2 打开“Microsoft ISA 安装向导”，在欢迎页中单击“下一步”按钮。在打开的“许可协议”向导页中点选“我接受许可协议中的条款”单选框，并单击“下一步”按钮。打开“客户信息”向导页，在此输入合法的客户信息和产品序列号，并单击“下一步”按钮。



输入合法的客户信息

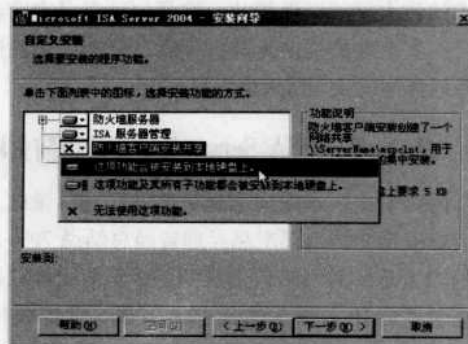
STEP 3 在打开的“安装类型”向导页中提供了三种安装类型，每种类型分别代表一种功能集合。一般情况下选择典型安装就行了，本例考虑到技术内容的充实性，这里点选“自定义”单选框，单击“下一步”按钮。



选择安装方案

STEP 4 打开“自定义安装”向导页，默认情况下向导只安装“ISA 服务器”和“ISA 服务器管理”两个组件。而“防火墙客户端安装共享”和用于控制垃圾邮件和邮件附件的“消息筛选程序”不会安装。如果用户想安装“消息筛选程序”，则需要首先在 ISA Server 服务器上安装 IIS 6.0 SMTP 服务。为了在后续操作中方便安装防火墙

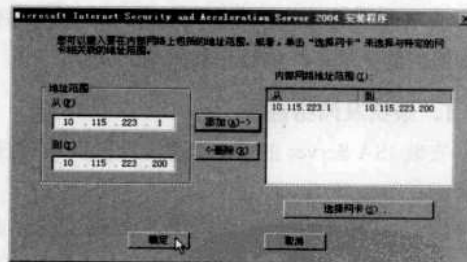
客户端，单击“防火墙客户端安装共享”选项左侧的下拉按钮，执行“这项功能会被安装到本地硬盘上”快捷命令。最后单击“下一步”按钮。



选择安装组件

STEP 5 打开“内部网络”向导页，在 ISA Server 中将“内部网络”定义为 ISA Server 服务器必须与之进行数据通信的可信网络，防火墙的系统策略会自动允许 ISA Server 服务器与内部网络进行有限制的通信。单击“添加”按钮。

STEP 6 在打开的地址范围对话框中需要设置内部网络的地址范围。在“地址范围”区域设置地址范围为从“10.115.223.1”到“10.115.223.200”，单击“确定”按钮。



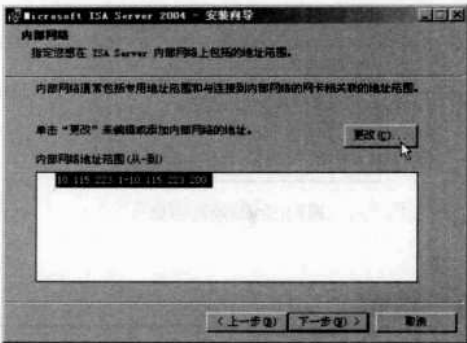
设置内部网络IP地址范围

注意

如果读者对路由表比较熟悉，可以在这一步操作中单击“选择网卡”按钮制定内部网络适配器。选中该选项后在后续操作中可能需要设置路由表，有兴趣的读者可以自行实验。

第十三章 局域网安全管理与维护

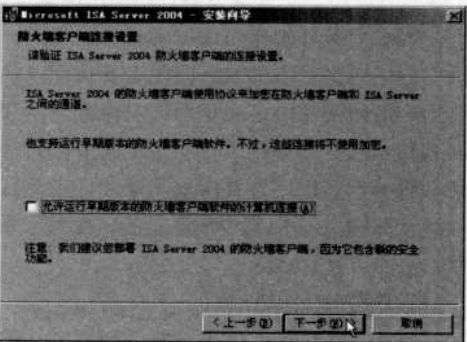
STEP 7 返回“内部网络”向导页，可以看到在“内部网络地址范围”列表中出现了刚刚添加的IP地址段。如果希望更改这个地址范围，可以单击“更改”按钮。确认无误后单击“下一步”按钮。



选则内部网络地址范围

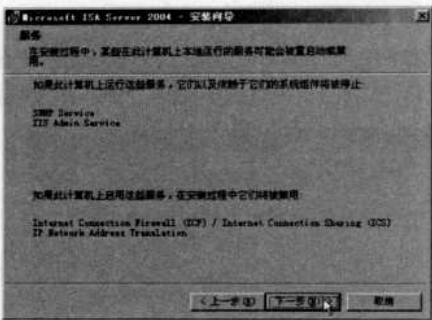
STEP 8 打开“防火墙客户端连接设置”向导页，如果用户的客户端计算机中安装了旧版本的ISA Server 防火墙客户端，则需要选取“允许运行早期版本的防火墙客户端软件的计算机连接”复选框。

由于ISA Server 服务器与旧版本的防火墙客户端软件之间采取不加密的方式进行连接，因此建议在客户端计算机中安装防火墙客户端。单击“下一步”按钮。



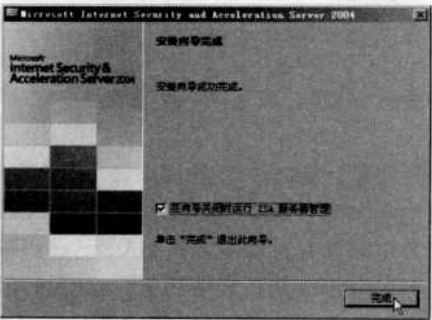
防火墙客户端连接设置

STEP 9 打开“服务”向导页，提示用户安装向导将重启和禁用本地计算机中的某些服务。直接单击“下一步”按钮即可。



提示某些服务将被禁止

STEP 10 最后打开“可以安装程序了”向导页，直接单击“安装”按钮开始安装。完成安装后单击“完成”按钮自动打开ISA Server 管理窗口。如果不能自动启动服务建议重新启动计算机。



完成安装

3. 安装防火墙客户端

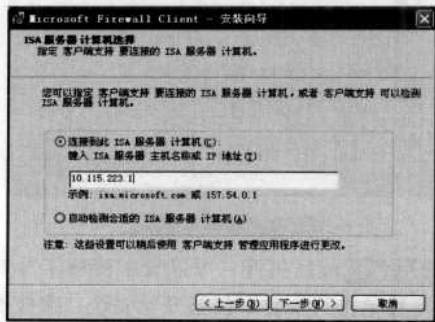
在上面的自定义安装中选取了“防火墙客户端安装共享”选项，局域网中的其它计算机可以通过UNC路径\\ServerName\\clients访问共享文件夹，防火墙客户端程序复制到本地计算机进行安装。ISA客户端的安装过程比较简单，下面简述如下：

STEP 1 运行安装程序“Setup.exe”进入“Microsoft Firewall Client 安装向导”，单击“下一步”按钮。打开“目标文件夹”向导页，单击“更改”按钮选择客户端安装目录（建议保持默认目录），并单击“下一步”按钮。

STEP 2 打开“ISA 服务器计算机选择”向导页，在向导页中指定防火墙客户端要连接的ISA服务器计算机。点选“连接到此ISA服务器”



计算机”单选框，并在其下的编辑框中输入 ISA 服务器的主机名或 IP 地址（本例输入 IP 地址“10.115.223.1”）。设置完毕单击“下一步”按钮。



指定ISA服务器计算机

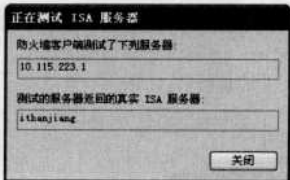
STEP 3 在打开的“可以安装程序了”向导页中单击“安装”按钮，打开“正在安装 Microsoft Firewall Client”向导页。可以通过进度条掌握安装进度，安装完毕直接单击“完成”按钮即可。

STEP 4 完成安装后防火墙客户端会自动在网络中检测 ISA Server 服务器并连接。如果防火墙客户端没有自动连接到 ISA Server 服务器，用户可以双击系统托盘中的客户端图标，打开“Microsoft Firewall Client for ISA Server”对话框。点选“手动选择 ISA 服务器”单选框，在编辑框中输入 ISA 服务器的 IP 地址或主机名，并单击“测试服务器”按钮。



手动检测ISA服务器

STEP 5 打开“正在测试 ISA 服务器”对话框，如果网络畅通会很快返回 ISA 服务器的主机名。依次单击“关闭/确定”按钮连接至 ISA Server 服务器。



返回ISA服务器信息



注意

在安装 Microsoft 防火墙客户端的计算机上不要安装其它的防火墙软件，否则将导致防火墙客户端无法检测到 ISA 服务器。同样，在安装 ISA Server 服务器的计算机上也不要安装其它的防火墙软件。

4. 允许本地主机和内部网络连接到Internet

ISA Server 服务器安装完毕以后会自动启用默认的防火墙策略规则，阻断所有内部用户（包括本地主机）与外部网络的连接。只有通过添加防火墙策略才能允许内部用户与外部网络进行通信。在 ISA Server 中，防火墙策略规则是由网络规则、访问规则和服务器发布规则三者组合而成的。其中网络规则定义了不同网络间是否能访问以及如何访问，而访问规则定义了用户对内部网络和外部网络的访问，服务器发布规则定义了如何让用户访问服务器。而用户要实现的是允许内部网络连接到 Internet，因此需要创建新的、凌驾于系统策略之上的访问策略。

(1) 查看系统策略规则

在安装 ISA Server 服务器时会创建默认的系统策略，系统策略允许 ISA Server 服务器访问与其相连接到的网络的特定服务。查看系统策略的方法为：

STEP 1 依次单击“开始/所有程序/Microsoft ISA Server/ISA 服务器管理”，打开“Microsoft Internet Security and Acceleration Server”窗口。

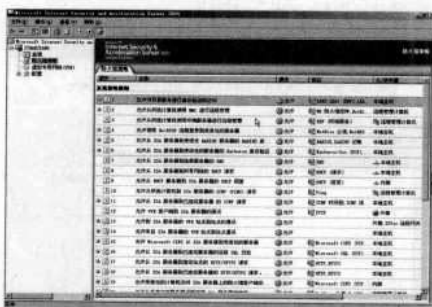
第十三章 局域网安全管理与维护

然后在左窗格中右键单击“防火墙策略”选项，执行“查看/显示系统策略规则”快捷命令。



显示系统策略规则

STEP 2 这时会在右窗格中显示系统策略规则的详细信息，用户可以看到这些规则几乎包含了 ISA Server 与内部网络和外部网络的所有通信类型，且大部分规则默认都是启用的。只有标有红色箭头的策略规则默认未启用。



系统策略规则详细信息

注意

系统策略规则和防火墙策略规则的区别：系统策略规则是 ISA Server 的默认规则，安装完成后自动生成并启用相关规则；而防火墙策略规则是用户自己创建的，用户根据实际需要可以灵活创建多种规则；系统策略规则优先于防火墙策略规则。

(2) 允许本地主机连接到 Internet

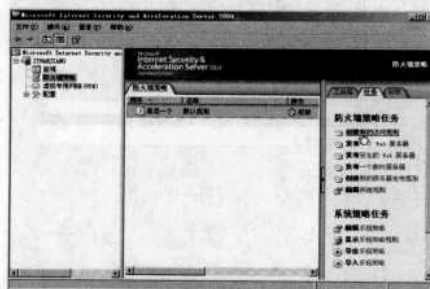
如何创建防火墙规则让本地主机访问 Internet 呢，其实用户只需创建一条访问规则即可轻松实现这一目的。

注意

在 ISA Server 服务器中附带了网络模版的功能，可以帮助用户方便地创建防火墙策略规则。不过本例只是创建一条简单的允许内部用户访问 Internet 所有服务的策略规则，使用模版其实还是较为繁琐的。而使用 ISA Server 提供的规则向导则会使这一过程显得更加轻松愉快。

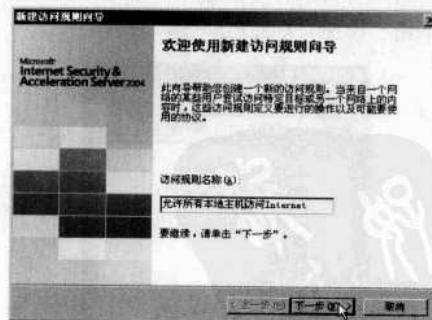
在 ISA Server 服务器中通过规则向导创建上述访问规则步骤如下所述：

STEP 1 打开 ISA Server 管理窗口，在任务窗格中单击“创建新的访问规则”超链接。



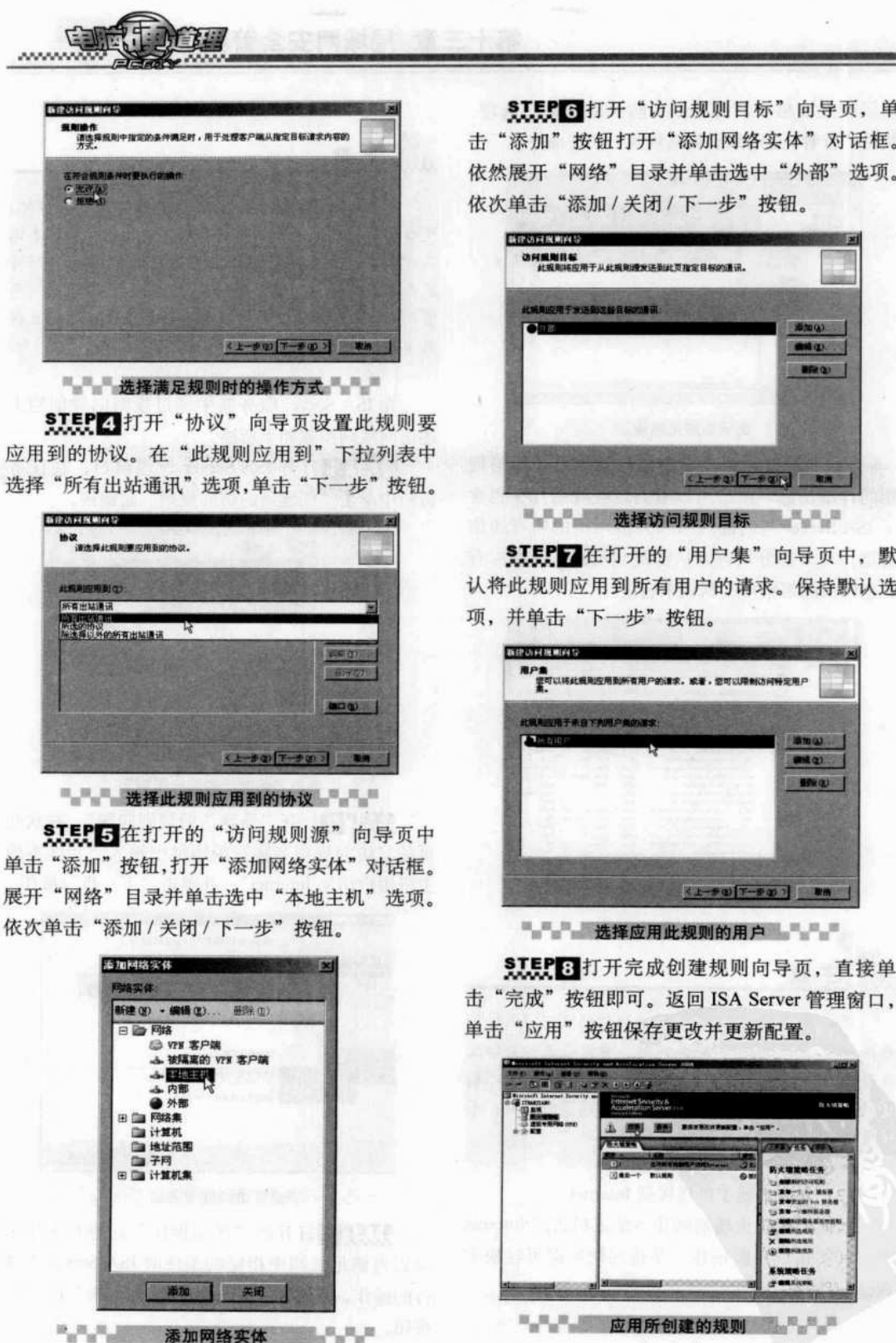
单击“创建新的访问规则”

STEP 2 打开“新建访问规则向导”，在欢迎页面的“访问规则名称”编辑框中输入“允许本地主机用户访问 Internet”，并单击“下一步”按钮。



设置访问规则名称

STEP 3 打开的“规则操作”向导页中用来设置当满足规则中指定的条件时 ISA Server 要执行的操作，点选“允许”单选框并单击“下一步”按钮。

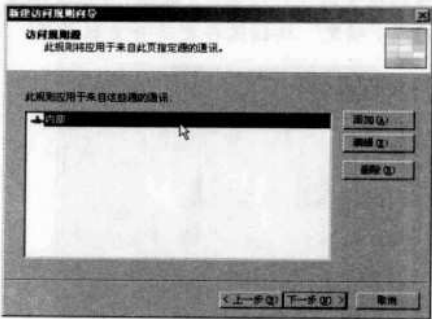


第十三章 局域网安全管理与维护

创建访问规则后，通过静态 IP 地址接入 Internet 的本地主机已经可以正常访问 Internet 了。如果 ISA Server 所在的服务器需要拨号才能接入 Internet，必须首先拨号接入 Internet 才行。

(3) 允许内部用户访问 Internet

为了使所有的内部用户也能够访问 Internet，需要再创建一条访问规则来实现。创建这条规则的方法跟上述步骤完全相同，只是在添加访问规则源的时候应当在“网络实体”对话框中选择“内部”选项。创建完成以后单击“应用”按钮使设置生效。



添加访问规则源

5. 使用模版创建防火墙策略

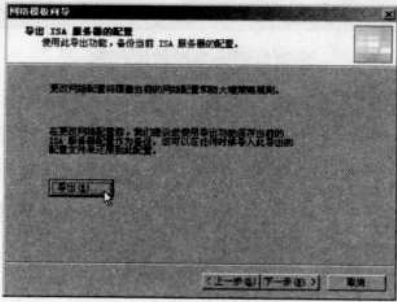
在 ISA Server 服务器中创建访问规则时，除了可以使用各种配置向导外，使用系统提供的网络模版也不失为一种快捷的方式。ISA Server 提供了 5 种模版，分别是“边缘防火墙”、“3 向外围网络”、“前端防火墙”、“后段防火墙”和“单一网络适配器”。其中边缘防火墙的作用是将网络连接至 Internet 并防止网络受到入侵，因此其适用范围最为广泛。下面以“边缘防火墙”模版为例介绍创建防火墙访问策略的方法，具体操作步骤如下所述：

STEP 1 打开 ISA Server 管理窗口，在左窗格中依次展开“ServerName/ 配置”目录，并单击选中“网络”选项。这时右侧的“任务窗格”默认打开“模版”选项卡，里面列出了系统内置的五种模版，单击“边缘防火墙”模版。



单击“边缘防火墙”模版

STEP 2 打开“网络模版向导”，在欢迎页中单击“下一步”按钮。在打开的“导出 ISA 服务器的配置”向导页中，如果用户以前没有保存过配置，则可以单击“导出”按钮保存当前配置。由于本例的 ISA Server 服务器是新配置的，因此单击“导出”按钮。



导出ISA服务器的配置

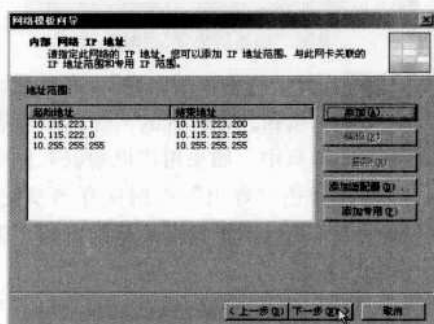
STEP 3 在打开的“导出配置”对话框中选择文件保存位置，并选取“ISA 服务器导出选项”区域的“导出用户权限设置”和“导出机密信息(将使用加密)”复选框，然后单击“导出”按钮。成功导出配置后单击“确定”按钮返回“导出 ISA 服务器的配置”向导页，并单击“下一步”按钮。



成功导出配置

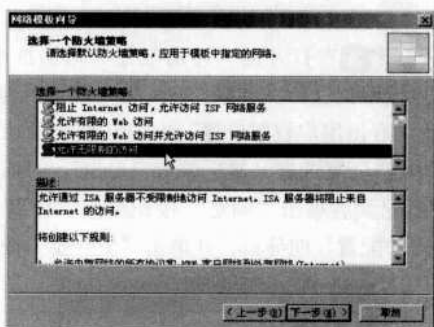


STEP 4 打开“内部网络 IP 地址”向导页，确认向导正确识别了内部网络的 IP 地址。在该向导页中，用户可以通过添加 IP 地址、添加适配器或添加专用地址来添加更多的 IP 地址。添加到“地址范围”列表框中的 IP 地址将被允许访问外部网络 (Internet)，确认内部 IP 地址范围无误后单击“下一步”继续。



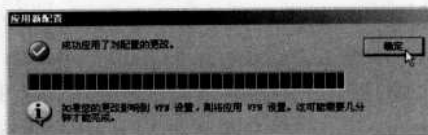
设置内部网络 IP 地址范围

STEP 5 打开“选择一个防火墙策略”向导页，在“选择一个防火墙策略”列表中单击选中一个防火墙策略。本例选中“允许无限制的访问”选项，该策略将允许内部网络和 VPN 客户端网络中的计算机无限制访问 Internet。设置完毕单击“下一步”按钮。



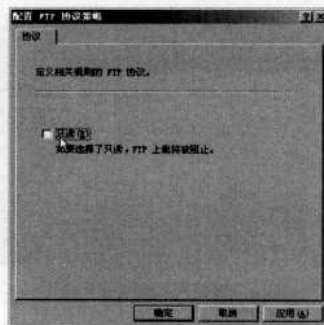
选择防火墙策略

STEP 6 在打开的完成向导页单击“完成”按钮，返回 ISA Server 管理窗口。在左窗格中单击“防火墙策略”选项，这时可以在右窗格中看到新建的策略规则。最后依次单击“应用 / 确定”按钮保存更改并更新配置。



应用新配置

大师点拨：出于安全考虑，ISA Server 服务器默认不允许 FTP 上传（即不能向位于外部网络的 FTP 服务器），用户必须手动取消 FTP 的“只读”属性才能实现 FTP 上传。在上述创建的“无限制的 Internet 访问”策略规则上单击右键，执行“配置 FTP”快捷命令。在打开的“配置 FTP 协议策略”对话框中取消“只读”复选框，并依次单击“确定 / 应用 / 确定”按钮保存更改并更新设置。



取消“只读”复选框

6. 启用缓存

ISA Server 服务器对于被经常请求访问的对象保存在磁盘缓存中以提高网络性能，用户可以通过配置缓存以确保其包含最常用的数据。在安装 ISA Server 服务器默认是禁用缓存的，这是因为在 ISA Server 服务器计算机的任何磁盘驱动器上都没有指定用于缓存的空间。当配置驱动器用于缓存时，通过指定在该驱动器上要使用的空间来启用缓存，并进一步配置缓存以指定可以缓存哪些内容。

只有启用缓存后用户才能够配置缓存规则。缓存规则通常是指当用户访问位于 ISA Server 服务器之后的站点时，是要直接访问站点中的内容还是从 ISA Server 服务器缓存中检索该内容。因此，缓存规则应用于站点而与源网络无关。

通过上面的叙述可以得知，启用缓存有两个

第十三章 局域网安全管理与维护

条件：一是设置缓存所用的驱动器，二是设置缓存规则。在 ISA Server 服务器中可以通过缓存规则设置向导来设置规则，这使得这一过程变得很容易。

(1) 设置缓存所用的驱动器

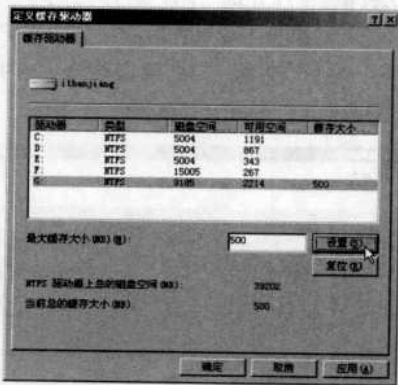
设置缓存所用的驱动器的步骤比较简单，具体操作步骤如下：

STEP 1 打开 ISA Server 管理窗口，在左窗格中依次展开“ServerName/配置”目录。可以看到“缓存”选项图标上有个向下的红色箭头，这表明没有启用缓存。然后右键单击“缓存”选项，执行“定义缓存驱动器”快捷命令。



执行“定义缓存驱动器”命令

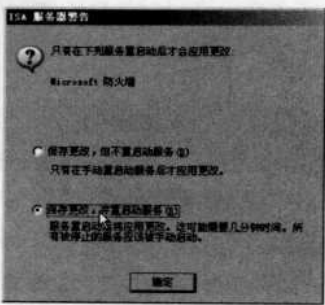
STEP 2 在打开的“定义缓存驱动器”对话框中，用户根据网络带宽及流量选择合适大小的磁盘分区。在“最大缓存大小”编辑框中输入要使用的磁盘空间大小（如“500”），并依次单击“设置/确定”按钮。



定义缓存驱动器

STEP 3 返回 ISA Server 管理窗口，单击“应

用”按钮。此时会弹出“ISA 服务器警告”对话框，提示用户需要重新启动“Microsoft 防火墙”服务才能应用启用缓存后的更改。点选“保存更改，并重启动服务”单选框，单击“确定”按钮。

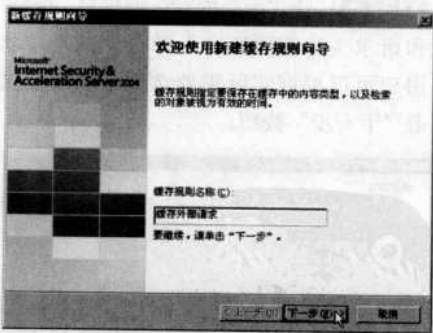


确定重新启动“Microsoft 防火墙”服务

(2) 设置缓存规则

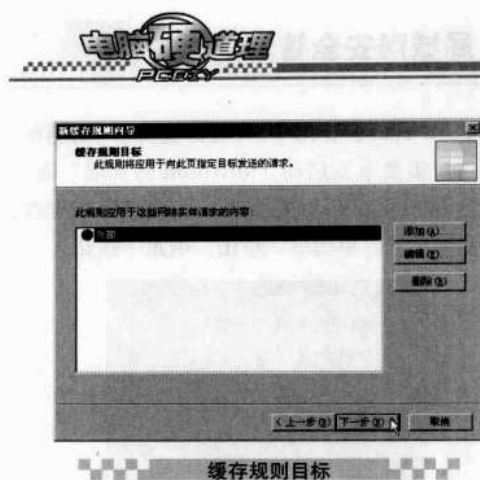
这时再次观察 ISA Server 管理窗口中的“缓存”选项，可以看到红色箭头已经消失了，这表明已经成功设置了缓存驱动器。接着需要设置缓存规则，以使缓存功能更符合用户的实际环境。

STEP 1 在“缓存”选项上单击鼠标右键，依次执行“新建/缓存规则”快捷命令。打开“新建缓存规则向导”，在欢迎页中输入缓存规则名称（本例输入“缓存外部请求”），并单击“下一步”按钮。

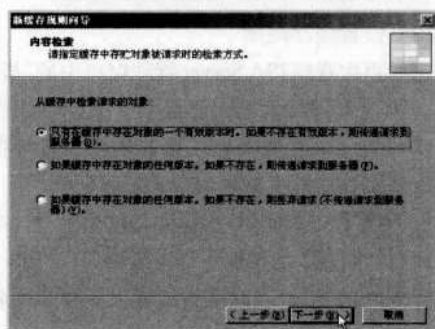


设置缓存规则名称

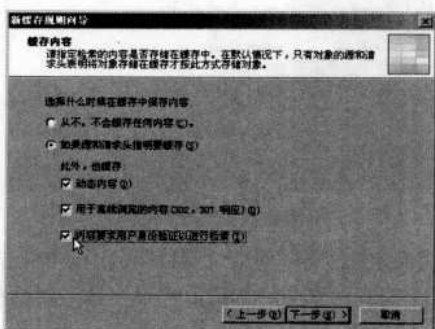
STEP 2 打开“缓存规则目标”向导并单击“添加”按钮。在打开的“添加网络实体”对话框中展开“网络”目录，双击“外部”选项并单击“关闭”按钮。返回“缓存规则目标”向导页，单击“下一步”按钮。



STEP 3 在打开的“内容检索”向导页中保持“只有在缓存中存在对象的一个有效版本时。”单选框的选中状态，直接单击“下一步”按钮。

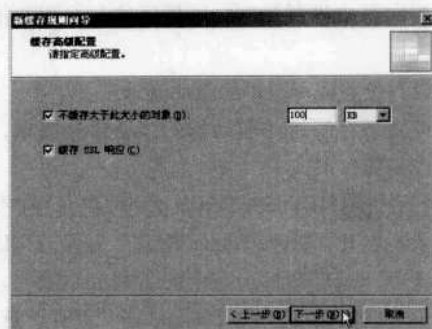


STEP 4 打开“缓存内容”向导页，保持“如果源和请求头指明要缓存”单选框的选中状态。另外用户可以根据实际需要选取下面的复选框，并单击“下一步”按钮。

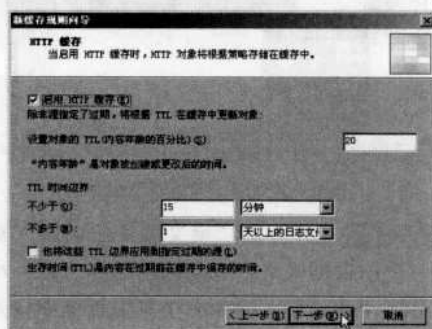


STEP 5 在打开的“缓存高级配置”向导页中选取“不缓存大于此大小的对象”复选框，然

后将对象大小设置为“100KB”。设置完毕单击“下一步”按钮。



STEP 6 打开“HTTP 缓存”向导页，如果启用 HTTP 缓存，则 HTTP 对象将根据策略存储在缓存中。保持默认设置并单击“下一步”按钮。



STEP 7 在打开的“FTP 缓存”向导页中以设置 FTP 对象是否存储在缓存中。由于 FTP 对象的体积一般比较大，因此建议取消“启用 FTP 缓存”复选框，并单击“下一步”按钮。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十三章 局域网安全管理与维护

STEP 8 最后单击“完成”按钮完成设置，返回 ISA Server 服务器窗口后单击“应用”按钮保存更改并更新设置，用户可以在右窗格中看到新建的缓存规则。



成功创建缓存规则

7. 系统监视轻轻松松

在基于 ISA Server 服务器和 Microsoft 防火墙客户端构成的防火墙体系中，监视系统和网络活动非常轻松。用户可以通过 ISA Server 服务器管理窗口中的“监视”节点来了解 ISA 服务器和防火墙客户端之间的会话、ISA 服务器的服务运行情况、进行连接性检查，并且可以通过日志来实时查询客户端的网络活动。

(1) 使用监视功能

打开 ISA Server 管理窗口，在右窗格中单击“仪表板”标签，在“仪表板”选项卡中可以清晰地看到 ISA Server 服务器当前系统和网络的运行情况。而在“会话”选项卡中则可以了解当前跟 ISA Server 服务器进行通信的客户端计算机信息。



仪表板选项卡

通过日志功能可以对防火墙客户端的网络活动状况了如指掌，用户可以通过编辑筛选器来指定日志查询条件。具体操作步骤如下所述：

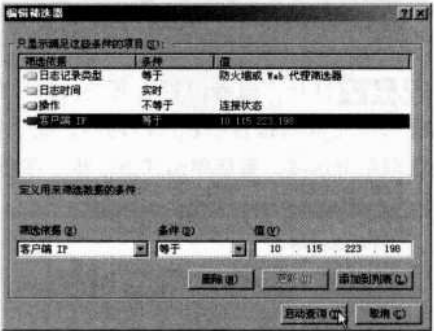
STEP 1 打开 ISA Server 服务器管理窗口，

在“监视”节点下切换至“日志”选项卡，并单击“编辑筛选器”超链接。



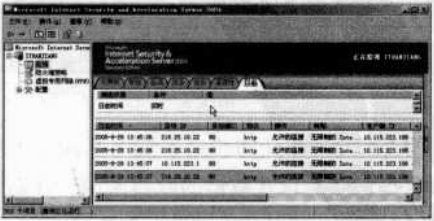
“日志”选项卡

STEP 2 打开“编辑筛选器”对话框，在“筛选依据”下拉列表选中“客户端 IP”选项，然后在“条件”下拉列表选中“等于”选项，并在“值”编辑框中输入目标防火墙客户端 IP 地址“10.115.223.198”，最后单击“添加到列表”按钮。接着在“只显示满足这些条件的项”列表选中刚才创建的筛选条件，单击“启动查询”按钮。



编辑筛选器

STEP 3 返回管理器窗口，在“日志”选项卡中可以实时获取防火墙客户端当前的网络活动信息。



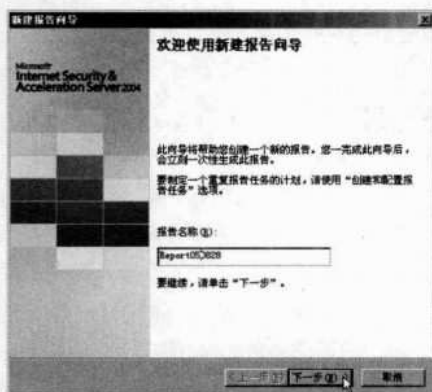
获取客户端网络活动信息

(2) 生成网络使用报告



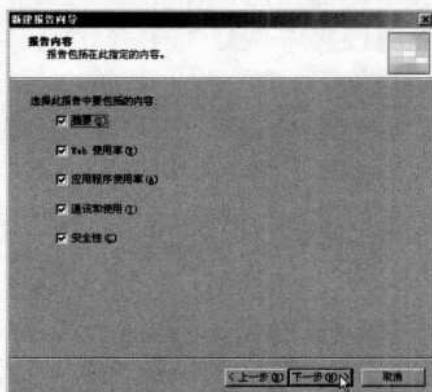
在实际的网络管理工作当中，经常需要向技术管理层呈交网络使用报告。借助 ISA Server 提供的“报告”功能，用户可以很轻松地生成网络使用报告，具体操作步骤如下所述：

STEP 1 在“监视”节点下单击“报告”标签，在“报告”选项卡中单击“生成新的报告”超链接。打开“新建报告向导”，在欢迎页向导中设置报告名称，并单击“下一步”按钮。



设置报告名称

STEP 2 打开“报告内容”向导页，用户可以选择要在生成的报告中包含的内容。默认情况下会选取全部选项，直接单击“下一步”按钮。



选择报告中包含的内容

STEP 3 在打开的“报告期间”向导页中可以设置报告中所包含数据的收集时段。分别设置“开始日期”和“结束日期”，并单击“下一步”按钮。

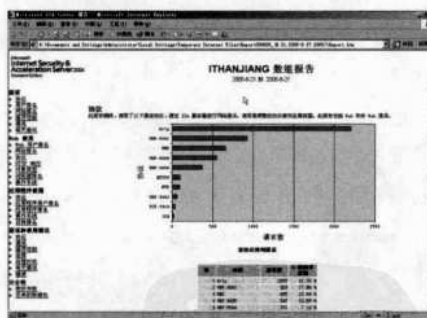
STEP 4 打开“报告发布”向导页，选取“将

报告发布到目录”复选框，并单击“浏览”按钮指定发布的报告的目录。然后选取“使用此账户发布”复选框，单击“设置账户”按钮选择账户。设置完毕单击“下一步”按钮。



指定报告发布的目录和账户

STEP 5 在打开的“发送电子邮件通知”向导页中直接单击“下一步”按钮，接着在完成向导页中单击“完成”按钮。返回“报告”选项卡，显示此报告的状态为“正在生成”。根据日志大小等待一段时间后，显示状态变为“完成”。双击此报告可以查看报告的详细内容。



查看报告详细内容

大师点拨：ISA Server 生成的网络使用报告内容非常详尽，覆盖了从用户使用的协议、用户访问流量、用户访问的站点、缓存的使用以及用户使用的浏览器和操作系统等多个方面。报告基于 HTML 格式，便于用户查看。

8. 发布内部网络中的服务器

在 ISA Server 服务器中可以轻松发布内部网络中的服务器，并且应用层过滤系统提高保证被

第十三章 局域网安全管理与维护

发布的内部服务器具有很高的安全性。下面以发布内部网络中的 Web 服务器和 FTP 服务器为例，谈一谈在 ISA Server 服务器中发布内部网络服务器的方法。

(1) 发布内部 Web 服务

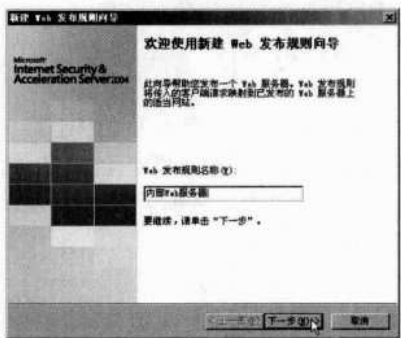
使用 ISA Server 服务器发布的内部 Web 服务器优点非常明显，那就是可以根据域名的不同将进入的 Web 访问请求转发到内部网络中不同的 Web 服务器上，具体设置步骤如下所示：

STEP 1 打开 ISA Server 服务器管理窗口，在左窗格中右键单击“防火墙策略”选项，依次执行“新建 /Web 服务器发布规则...”快捷命令。



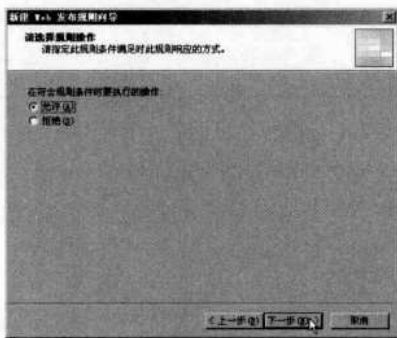
执行“Web 服务器发布规则”命令

STEP 2 打开“新建 Web 发布规则向导”，在欢迎向导页中设置 Web 发布规则名称（如“内部 Web 服务器”），并单击“下一步”按钮。



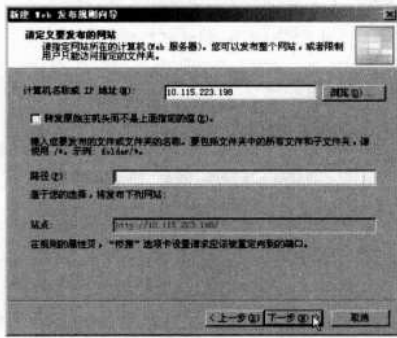
设置 Web 发布规则名称

STEP 3 在打开的“请选择规则操作”向导页中，需要指定当满足此规则条件时规则的响应方式。保持“允许”单选框的选中状态，并单击“下一步”按钮。



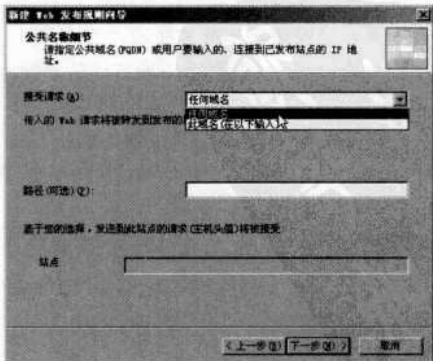
选择规则操作

STEP 4 打开“请定义要发布的网站”向导页，在“计算机名称或 IP 地址”编辑框中输入准备发布的内部 Web 服务器的 IP 地址或主机名称。其它选项保持默认状态，单击“下一步”按钮。



指定内部 Web 服务器

STEP 5 在打开的“公共名称细节”向导页中，用户可以设置域名以指向内部 Web 服务器。本例在“接受请求”下拉列表中选择“任何域名”选项，并单击“下一步”按钮。



设置域名信息

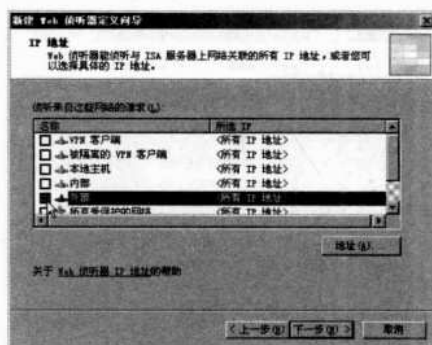


注意

用户可以通过创建多条 Web 发布规则，以便把不同的域名转发到不同的内部 Web 服务器上，从这个地方也能体现出 ISA Server 服务器的功能强大。

STEP 6 打开“选择 Web 侦听器”向导页，单击“新建”按钮打开“新建 Web 侦听器定义向导”。在欢迎向导页中设置 Web 侦听器名称(如“侦听外部 80 端口”)，并单击“下一步”按钮。

STEP 7 打开“IP 地址”向导页，在“侦听来自这些网络的请求”列表中选择“外部”选项，单击“下一步”按钮。



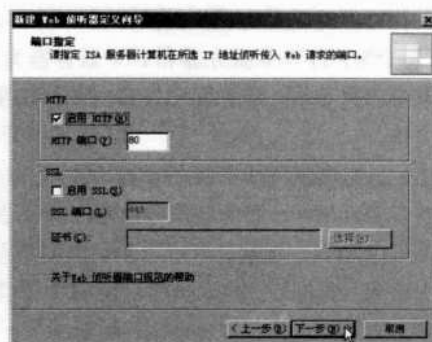
选择侦听的目标IP地址



注意

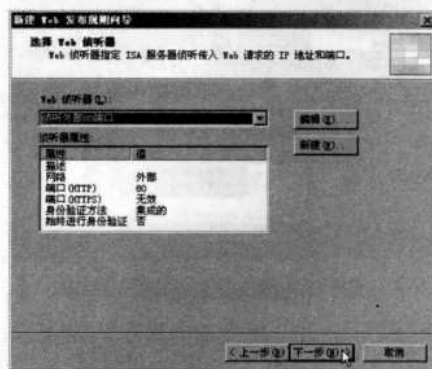
一般的 NAT (网络地址转换) 工具只能做到对外部网络发布内网的服务器，外部用户可以访问内部 Web 服务器，内部用户不能直接通过内部 Web 服务器发布的外部 IP 地址来访问发布的内部 Web 服务器。而 ISA Server 服务器则能够做到这一点，可以通过侦听内部客户的请求让内部客户通过内部 Web 服务器发布的外部 IP 地址来访问发布到外部的内部服务器。

STEP 8 在打开的“端口指定”向导页中，用户需要指定 ISA Server 在所选的 IP 地址上侦听传入 Web 请求的端口。使用 HTTP 默认的“80”端口，依次单击“下一步/完成”按钮完成创建。



指定端口

STEP 9 返回“选择 Web 侦听器”向导页，在“Web 侦听器”列表中已经出现了所创建的 Web 侦听器，并默认处于选中状态。单击“下一步”。



选择Web侦听器

STEP 10 打开“用户集”向导页，默认情况下该规则将应用于来自所有用户的请求。依次单击“下一步/完成”按钮完成发布规则向导，最后单击“应用”按钮保存更改并更配置。

至此，外部用户已经可以通过访问 ISA Server 服务器拥有的 IP 地址（或绑定的域名）来访问内部网站了。

(2) 发布内部 FTP 服务

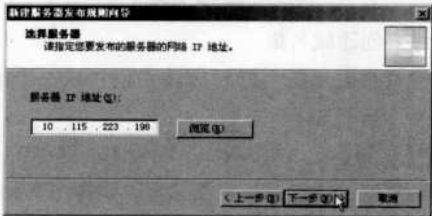
FTP 服务可以说是局域网或 Internet 中应用最广泛的网络服务之一，而且基于安全性考虑，很多 FTP 站点开放的 FTP 端口不是标准的 TCP 21 端口。通过 ISA Server 服务器发布向导，用户能够轻松发布标准端口或非标准端口的内部 FTP 服务。以发布非标准端口的 FTP 服务为例，具体操

第十三章 局域网安全管理与维护

作步骤如下：

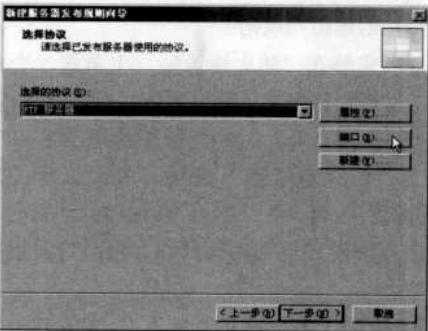
STEP 1 打开 ISA Server 服务器管理窗口，在左窗格中右键单击“防火墙策略”选项，依次执行“新建 / 服务器发布规则...”快捷命令。打开“新建服务器发布规则向导”，在欢迎向导页中设置服务器发布规则名称（如“发布内部 FTP 服务”），并单击“下一步”按钮。

STEP 2 在打开的“选择服务器”向导页中输入内部 FTP 服务器的 IP 地址（如“10.115.223.198”），并单击“下一步”按钮。



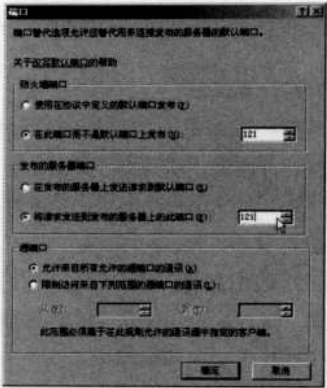
选择服务器

STEP 3 打开“选择协议”向导页，在“选择的协议”下拉列表中选中“FTP 服务器”选项，并单击“端口”按钮。



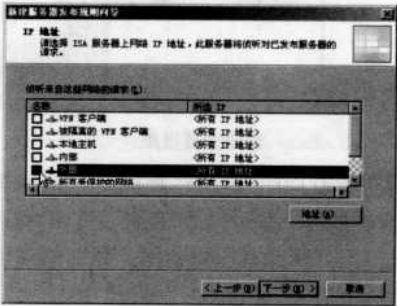
选择协议

STEP 4 在打开的“端口”对话框中，点选“防火墙端口”区域的“在此端口而不是默认端口上发布”单选框，并在右侧的微调框中输入一个自定义的端口（如“121”）。接着点选“发布的服务器端口”区域的“将请求发送到发布的服务器上的此端口”单选框，并根据实际情况设置端口。设置完毕依次单击“确定 / 下一步”按钮。



设置端口

STEP 5 打开“IP 地址”向导页，在“侦听来自这些网络的请求”列表选取“外部”复选框，并单击“下一步”按钮。



选择要侦听的IP地址

STEP 6 在完成向导页中单击“完成”按钮，返回管理窗口后单击“应用”按钮保存更改并更新配置。至此，内部 FTP 服务已经成功发布，外部用户可以使用 ISA Server 服务器拥有的公网 IP 地址（或绑定的域名）和设置的防火墙端口来访问该内部 FTP 站点。

13.1.3 ISA Server应用案例

上面谈了使用 ISA Server 服务器部署企业防火墙的几个重要技术点，那么 ISA Server 在实际的网络管理过程中有什么作用呢？相信下面的两个案例将为用户带来更实际的感受。

1. 限制特定计算机访问指定网站

限制用户上网是应用最频繁的网络管理工作之一，在 ISA Server 服务器中可以轻松实现这一

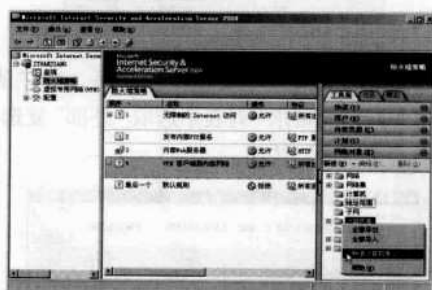


目的。以限制特定计算机访问指定网站为例简述如下：

(1) 创建计算机集

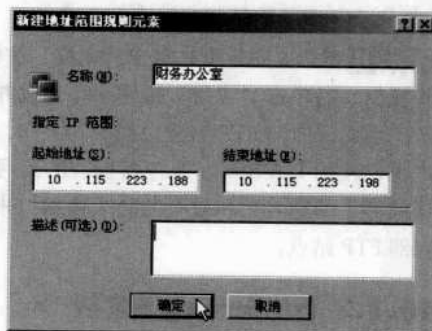
首先需要将限制上网的目标计算机创建成一个计算机集，具体操作步骤如下所述：

STEP 1 打开 ISA Server 服务器管理窗口，并在左窗格中选中“防火墙策略”选项。在任务窗格中切换至“工具箱”选项卡，并展开“网络对象”面板。然后右键单击“计算机集”选项，执行“新建计算机集”快捷命令。



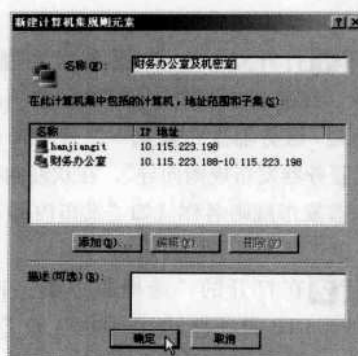
新建计算机集

STEP 2 打开“新建计算机集规则元素”对话框，依次单击“添加/地址范围”按钮，打开“新建地址范围规则元素”对话框。分别输入规则名称和 IP 地址范围，并单击“确定”按钮。



新建地址范围规则元素

STEP 3 返回“新建计算机集规则元素”对话框，可以再次单击“添加”按钮新建另外的计算机规则元素。完成添加后在“新建计算机集规则元素”对话框中设置计算机集名称，并依次单击“确定/应用”按钮。



完成创建的计算机集

(2) 创建域名集

接着将限制访问的目标站点创建成一个域名集，操作步骤如下：

STEP 1 在“网络对象”面板中右键单击“域名集”选项，执行“新建域名集”快捷命令。

STEP 2 打开“新建域名集策略元素”对话框，单击“新建”按钮新建一个域名，将域名命名为限制访问的目标站点域名（如 www.ithanjiang.com）。然后输入规则名称，设置完毕依次单击“确定/应用”按钮。

(3) 创建访问规则

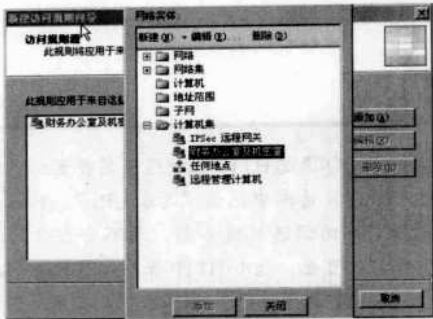
最后需要在“防火墙策略”中新建一个访问规则，以阻止特定的计算机集访问指定的域名集。

STEP 1 在 ISA Server 服务器管理窗口中右键单击“防火墙策略”选项，依次执行“新建/访问规则”快捷命令。打开“新建访问规则向导”，在欢迎页中设置规则名称（如“限制访问指定站点”）。

STEP 2 打开“规则”向导页，默认选取“拒绝”单选框，直接单击“下一步”按钮。在“协议”向导页中，将“此规则应用到”设置为“所有出站通讯”。

STEP 3 在打开的“访问规则源”向导页中单击“添加”按钮，打开“添加网络实体”对话框。在该对话框中展开“计算机集”，双击“财务办公室及机要室”选项，然后单击“关闭”按钮。

第十三章 局域网安全管理与维护



设置访问规则源

STEP 4 在打开的“访问规则目标”向导页中单击“添加”按钮，然后在“添加网络实体”对话框中展开“域名集”目录，并双击目标站点的域名。依次单击“关闭/下一步”按钮完成创建。

STEP 5 打开“用户集”向导页，保留默认的“所有用户”并依次单击“下一步/完成/应用”按钮使设置生效。

通过上述设置，IP 地址符合地址范围规则的计算机将被禁止访问 www.ithanjiang.com 站点。

2. 限制内部用户登录QQ

QQ 可以支持基于 UDP、HTTP 和 HTTPS 三种协议的登录方式，并且能够使用 HTTP 代理，在一定意义上可以断言：只要网络中允许 HTTP 协议，那么 QQ 就可以登录。正是因为 QQ 登录的特点，使得基于包过滤的防火墙（包括硬件防火墙和软件防火墙）均不能完全限制 QQ 登录。随着 ISA Server 服务器深层 HTTP 检查机制的出现，限制内部用户登录 QQ 变得简单起来。

为了能够成功限制 QQ 登录，了解 QQ 的登录过程非常必要。QQ 的登录过程大致分为几步：

- (1) 向 QQ 服务器群的 8000 端口发送 UDP

数据包，选择回复最快的服务器作为登录服务器；

(2) 如果没有服务器回复 UDP 数据包，则使用 TCP 80/443 端口来进行连接。

由此可见，QQ 能够通过 HTTP 方式直接登录。但一般情况下不能在网络中禁用 HTTP，因为这将导致内部用户不能浏览网页。因此限制 QQ 登录的最好办法是禁止内部用户访问 QQ 登录服务器的 IP 地址。不过 QQ 还可以使用 HTTP 代理登录，所以还要在 ISA Server 服务器的 HTTP 深层检查机制中设置限制 QQ 登录的 HTTP 连接。

(1) 禁用 QQ 登录服务器 IP 地址

禁用 QQ 登录服务器 IP 地址的方法跟限制特定用户访问指定网站的方法基本相同，同样是通过创建 QQ 计算机集和域名集，并创建访问规则来实现限制目的。在这一操作中关键需要获取 QQ 登录服务器的完整 IP 地址列表。用户可以在 QQ 客户端“系统设置”的“登录设置”面板中搜集 QQ 登录服务器的 IP 地址。



搜集QQ登录服务器IP地址

表 13-1 中列出了比较常用的 QQ 登录服务器 IP 地址，读者可以参考并增加。

表13-1

UDP 8000端口服务器				
61.134.238.135	61.134.238.136	61.134.238.156	61.134.238.150	61.131.194.203
61.131.194.200	61.131.194.224	202.104.129.251	202.104.129.254	202.104.129.252
202.104.129.253	202.96.170.166	202.96.170.164	202.96.170.163	
218.18.95.221	219.133.45.15	219.133.40.216	218.18.95.209	
TCP 80/443端口服务器				
218.17.209.23	218.18.95.153	61.131.194.227	218.18.95.171	218.18.95.221
会员VIP HTTP 443端口安全连接服务器				
218.17.209.42				



(2) 禁止 QQ 使用 HTTP 代理登录

通过限制内部用户访问 QQ 登录服务器 IP 地址，QQ 已经不能通过 UDP 方式进行登录。下面通过 ISA Server 服务器的 HTTP 深层检查机制来配置 HTTP 策略，从而禁止 QQ 使用 HTTP 代理登录。

STEP 1 在“防火墙策略”节点下右键单击允许 QQ 使用 HTTP 代理的策略规则（如“无限制的 Internet 访问”），执行“配置 HTTP”快捷命令。



配置 HTTP

STEP 2 打开“为规则配置 HTTP 策略”对话框，切换到“签名”选项卡并单击“添加”按钮。在打开的“签名”对话框中，设置签名搜索名称（如“禁用 HTTP 代理”）。在“签名搜索条件”区域指定查找范围为“请求 URL”，在“指定要阻止的签名”区域输入签名“tencent.com”。该设置使得 ISA Server 服务器找到该签名后将阻止这个连接，最后单击“确定”按钮。



设置签名属性

STEP 3 返回服务器管理窗口，单击“应用”按钮保存更改并更新配置。现在 QQ 已经无法通

过代理服务器登录。



只有在 QQ 通过 HTTP 代理服务器登录的时候才会在 HTTP 连接请求中包含“请求 URL”，如果是直接通过 HTTP 协议连接服务器，则不会包含“请求 URL”字段。可见，这个 HTTP 深层过滤机制只能针对 QQ 使用 HTTP 代理登录的情况，因此必须结合“禁用 QQ 服务器群”的防火墙策略规则一起使用。

13.2 系统漏洞检查与修补

借助于 Internet，一种新类型病毒可以在短短的几天时间内横扫全球。而且绝大多数病毒都隐身于 Web 服务和 E-mail 服务中，更是令人防不胜防。在拥有庞大数量计算机的网络中，一味的被动防御或杀毒并不是万全之策，系统漏洞的检查与修补就显得更为重要。

常见的检测系统漏洞的方法有很多，如前期准备，建立安全模型、源代码分析、二进制代码分析等等。不过这些方法要求过高，对于普通用户来说，可操作性不大。本例介绍一款微软推出的名为 Microsoft Baseline Security Analyzer (MBSA，以下简称 MBSA) 的工具软件，此软件可以很方便地让系统管理员了解和修正 Windows 2000/XP 的安全漏洞。

13.2.1 关于 MBSA

MBSA 可以扫描本机、多台电脑以及整个局域网的安全设置和系统漏洞。包括以下项目：检查是否安装修补程序、是否启动账户登录和退出，是否开启 Guest 使用者的账户、是否启动了不需启动的网络服务等；检查是否安装了 IIS Lockdown Tool、是否安装了 IIS 的安全修补程序，即检查 IIS 系统的安全设置；检查 SQL Server 的系统安全设置；检查 Internet Explorer 的设置；检查 OE/Outlook 的安全方面设置；检查 Microsoft Office 2K/XP 的 MACRO 安全设置等。

第十三章 局域网安全管理与维护

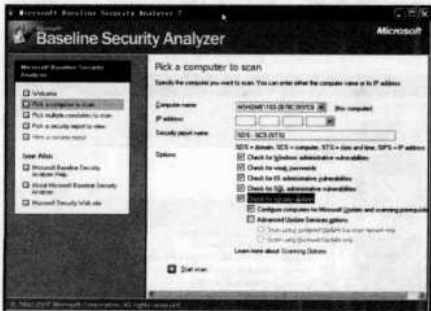
13.2.2 安装MBSA

MBSA 的安装比较简单，直接运行“MBSASetup-EN-20”程序进入安装引导。同意安装协议后连续单击“Next”按钮即可完成安装，此间涉及“Place shortcut on the desktop”（在系统的桌面建立快捷连接）、“Show Readme file after installation”（安装完程序后显示相关的文档资料）、“Launch application after installation”（安装完程序后立刻执行程序）的选择，建议保留软件默认设置，最后单击“Finish”按钮完成安装。

13.2.3 检查系统漏洞并修补

MBSA 可以检查单个电脑的安全漏洞，也可以一次检查一组 IP 地址中的所有电脑的网络安全设置。下面谈谈如何来检查系统漏洞。

STEP 1 运行 MBSA 软件，在右边的目录按下“Scan a computer”，然后在“Computer Name”中输入你的机器名称，或者在“IP Address”中输入要扫描机器的 IP 地址，而且需选取“Check for Windows administrative vulnerabilities”（检查 Windows 的系统漏洞）、“Check for weak passwords”（检查弱口令）、“Check for IIS administrative vulnerabilities”（检查 IIS 的系统漏洞）、“Check for SQL administrative vulnerabilities”（检查 SQL 程序的系统漏洞）、“Check for security updates”（检查安全升级）。“Security report name”保留默认值即可，单击“Start Scan”按钮，开始检查系统漏洞。



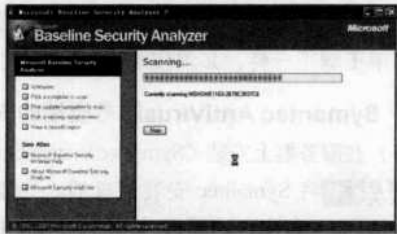
扫描设置



注意

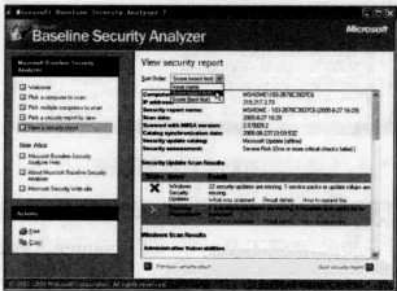
第一次执行扫描的时候，软件要更新一下数据，这个过程相对来说比较漫长，而且没有任何指示。大约两三分钟过后，软件就开始全面地扫描系统了。

STEP 2 扫描结束，并形成报告。这个过程大约需要五分钟，检查完毕后，会出现一份系统安全方面的报告，详细说明系统有什么安全漏洞，并指出如何修补或更改设置。



扫描报告

STEP 3 根据扫描报告，修复系统漏洞。单击“Result details”按钮，就会出现一个详细报告的对话框。



详细报告

STEP 4 单击“Download”按钮即可将系统没有安装的补丁从微软网站下载下来，然后安装即可完成系统漏洞的修复。

随着 Windows 系统漏洞不断发现，电脑病毒更加变本加厉地肆虐着每一台电脑。加上网络上流通的黑客工具更是给 Windows 系统造成了巨大的危害。MBSA 虽然可以很方便地对系统的漏洞进行扫描并提供解决方案，但需要手动进行修复。



13.3 病毒、黑客防范

每年由病毒和黑客攻击而导致的各种显性和隐性的损失，可以说是天文数字。在拥有庞大数量计算机网络中，仅仅安装少量的防病毒软件根本无济于事，因为只要有感染病毒的计算机存在，那么网络中就永无宁日。因此，网络病毒的查杀就显得更为重要。

13.3.1 网络病毒的防范

以诺顿企业版 10.0 为例，介绍一下网络版杀毒软件的安装，以及病毒的查杀和预防。诺顿企业版和单击版不一样，必须按照正确的顺序安装：

1. Symantec AntiVirus服务器端的安装

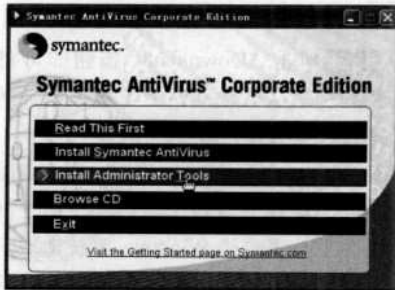
(1) 在服务器上安装“Symantec System Center”

STEP 1 将 Symantec 安装光盘插入光驱，光盘会自动运行，若未自动运行，可运行光盘中的“setup”文件打开该窗口。



自动运行界面

STEP 2 单击“Install Administrator Tools”，选择要安装的管理工具——“Symantec System Center”。



安装界面

STEP 3 单击“Install Symantec System Center”，打开 Symantec System Center 安装向导。一路“Next”即可完成。完成安装后，系统会提示重新启动系统。



注意

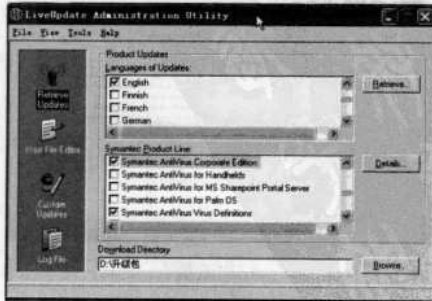
Symantec System Center 用于管理 Symantec 产品和警报，可以安装在 Windows NT/2K/XP/2003 的操作系统上，并要求系统中必须安装有 Internet Explorer 5.5 以上版本。如果版本低于 5.5 则会出现提示框，要求将 IE 升级至 5.5 以上版本。

(2) 安装“LiveUpdate Administrator”

STEP 1 运行 Symantec，依次单击“Install Administrator Tools/Install LiveUpdate Administrator”，会出现“是否安装 LiveUpdate Administrator 询问对话框”。

STEP 2 安装过程比较简单，完成后显示“Setup Complete”对话框。选中“Launch Live Update Administrator Utility”复选框，以便立即开始病毒库的更新。

STEP 3 单击“Finish”，显示“LiveUpdate Administrator Utility”对话框。在左侧栏中选择“Retrieve Updates”图标，在右侧“Product Updates”栏中选中“English”复选框，在“Symantec Product Line”栏中选中“Symantec AntiVirus Corporate Edition”和“Symantec AntiVirus Virus Definitions”复选框，并在“Download Directory”框中指定保存下载文件的文件夹。



升级设置

第十三章 局域网安全管理与维护

注意

由于本文安装的诺顿企业版是英文版，所以在右侧“Product Updates”栏中选中“English”复选框，在“Symantec Product Line”栏中选中两个选项一个为杀毒引擎一个为病毒库。

STEP 4 单击“Retrieve...”按钮显示“LiveUpdate”对话框，系统自动完成升级的过程。

(3) 安装“Quarantine Console”

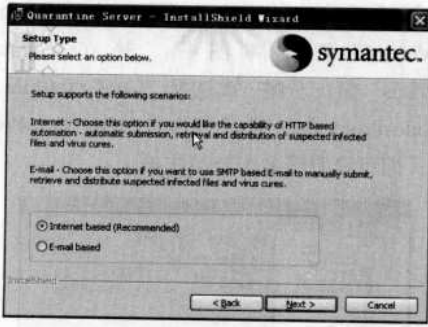
将光盘放入光驱中运行，在安装界面上单击“Install Quarantine Console”按钮，根据系统提示即可成功安装，并重新启动计算机。

注意

中央隔离区由隔离区服务器和隔离区控制台构成。隔离区服务器既可以与控制台安装在同一台计算机上，也可以不安装在同一计算机上。安装“Central Quarantine”时需先安装“Quarantine Console”，再安装隔离区服务器。

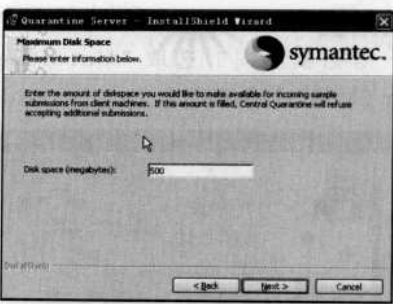
(4) 安装“Central Quarantine”

STEP 1 在安装界面上，点选“Install Central Quarantine”单选框，显示“Setup Type”对话框，这里如何选择取决于读者的网络。



“网络类型”对话框

STEP 2 单击“Next”按钮，显示“Maximum Disk Space”对话框。指定用于保存客户机提供样本可占用的最大磁盘空间，默认值为 500MB。



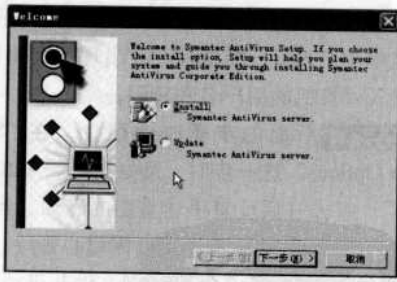
“最大磁盘空间”对话框

STEP 3 单击“Next”按钮显示“Contact Information”对话框，用于定制客户信息。在相应的字段中分别键入 Company Name, Account Number, Contact Name, Contact Telephone, Contact E-mail Address。

STEP 4 单击“Next”按钮显示“Web Communication”对话框，更改“Gateway Name”（或选择默认状态）。单击“Next”按钮，显示“Quarantine Server Installer Information”对话框，单击“Yes”，重新启动计算机。

(5) 安装“Deploy AntiVirus Server”

STEP 1 运行光盘，点选“Install Symantec AntiVirus”单选框，单击“Deploy AntiVirus Server”按钮即可显示安装向导。



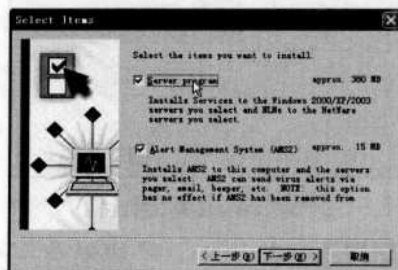
欢迎向导

注意

第一次安装可以在“Welcome”对话框中选择“Install Symantec AntiVirus Server”；日后 Symantec AntiVirus 服务器出现故障，可使用“Update Symantec AntiVirus Server”进行修复。



STEP 2 单击“Next”按钮，在“Select Items”对话框上同时选取“Alert Management System (AMS2)”的复选框。



安装向导



注意

在安装“Deploy AntiVirus Server”时，建议同时安装“Alert Management System (AMS2)”程序。这样一来既可以更灵活地选择哪些计算机可进行更为高级的警报操作；又可以在更改一级服务器时，不需要在新的服务器上重新安装 AMS2。

STEP 3 单击“下一步”按钮，显示“Select Computers”对话框。从左侧“Network”列表中选择安装“AntiVirus Server”的计算机，单击“Add”按钮将其添加至“Destination”列表中。一般情况下，当单击“Add”按钮时，会出现一个对话框，要求键入计算机的用户名和密码。

STEP 4 后面的步骤改动很少。在“Server Startup Options”这一步时，最好选择“Automatic startup”，省去日后反复手动重启的麻烦。当到达“Setup Progress”这一步，读者需耐心等待，因为此时系统开始向各服务器中复制文件并进行安装，根据网络带宽不同，所耗时间也不相同。安装完成后，单击“Close”按钮关闭该向导。

2. 病毒库和杀毒引擎升级

STEP 1 双击任务栏托盘区中的 Symantec AntiVirus 黄色盾牌图标，或单击右键并从菜单中选择“Open Symantec AntiVirus”选项。在“Symantec AntiVirus”对话框中填写“Username”和“Password”。单击“OK”按钮，显示“Symantec

AntiVirus”窗口。



手动更新

STEP 2 单击“LiveUpdate”按钮，显示“LiveUpdate”向导，用来升级 Symantec 病毒库和杀毒引擎。更新安装完成后，系统会列出更新的内容，单击“完成”按钮，更新完毕。

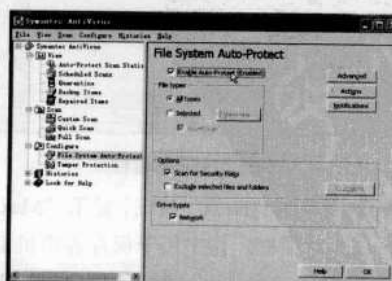


注意

在升级过程中，某些网络需要设置代理才可以正常的升级。读者只需将 IE 设置代理即可，Symantec AntiVirus 默认设置使用 IE 代理。

3. 配置自动防护

Symantec AntiVirus 可以自动防护计算机，无论是访问、复制、保存、移动或者关闭文档或文件、运行应用程序还是访问 Internet，Symantec AntiVirus 都将严密进行监视，一旦发现病毒立即进行处理。双击任务栏托盘区中的 Symantec AntiVirus 黄色盾牌图标，并在“Symantec AntiVirus”窗口左侧一次选择“Configure/File System Auto-Protect”，显示 File System Auto-Protect 窗口，即可设置服务器自动防护。



服务器自动防护

第十三章 局域网安全管理与维护

4. 安装Symantec AntiVirus客户端

安装 Symantec AntiVirus 客户端的方式有很多种，比较常见的有借助 Web 服务器分发和安装，从服务器上的客户端磁盘映像运行客户端安装程序，直接从光盘上安装，使用登陆脚本完全自动进行客户端安装和更新等等。



注意

在客户端计算机上安装 Symantec AntiVirus 客户端之前，应先将 Symantec AntiVirus 服务器程序安装到一台或多台服务器上，并在客户端安装时选择“接收管理”模式。

在网络环境中必须安装网络版的杀毒软件，强制为每台计算机安装病毒防护系统，并为每个客户端升级病毒库和杀毒引擎，从而达到防患于未然的目的。

13.3.2 瑞星杀毒软件

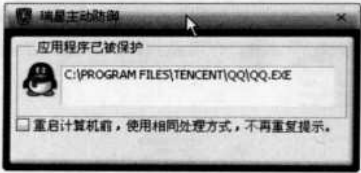
在病毒木马泛滥的今天，互联网上“裸奔”显得不太现实，杀毒软件成为用户安装好系统后最先安装的软件。

作为一款老牌的杀毒工具，瑞星最大的亮点就是“主动防御”和“即时升级”，可以为你的电脑构建铜墙铁壁。

1. 主动防御保护你的电脑

主动防御是近年来杀毒软件一直在提的一个概念，主动防御技术使得杀毒软件可以轻松阻止恶意程序执行，可以弥补传统杀毒软件的“特征码查杀”和“监控”的不足，可以在病毒发作时进行主动而有的防范。

运行瑞星杀毒软件，我们首先就感受到主动防御带给电脑的保护，由于笔者电脑中的 QQ 是随系统一起自动启动，系统启动完毕后，我们看到瑞星弹出一个提示，显示 QQ 程序已经被瑞星保护起来。



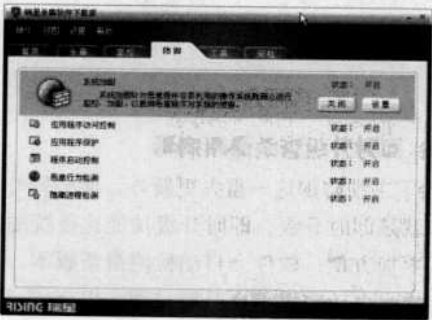
瑞星主动防御

而对于有些瑞星不能完全识别的软件，瑞星则会将决定权交给用户，比如运行超级旋风，瑞星则提示这是一个未签名的程序，让用户选择处理方式，对以可靠的程序，可以选择“总是允许”，这样，下次再运行该软件时，瑞星就会将程序保护起来。



允许程序运行

打开瑞星杀毒软件，点击“防御”选项，这里可以看到，主动防御中包括系统加固、应用程序访问控制、应用程序保护、程序启动控制、恶意行为检测和隐藏进程检测六大功能。



防御功能

点击其中任意一项中的“设置”按钮，可以进行更为详细的规则设置，这里不再详细介绍。



瑞星的主动防御定义三个层次：

第一层：资源访问控制通过对系统资源（注册表、文件、特定系统 API 的调用、进程启动）等进行规则化控制，阻止病毒、木马等恶意程序对这些资源的使用，从而达到抵御未知病毒、木马攻击的目的。

第二层：资源访问扫描层（传统的文件监控、邮件监控等）

通过监控对一些资源，如文件、引导区、邮件、脚本的访问，并使用拦截的上下文内容（文件内存、引导区内容等）进行威胁扫描识别的方式，来处理已经经过分析的恶意代码。

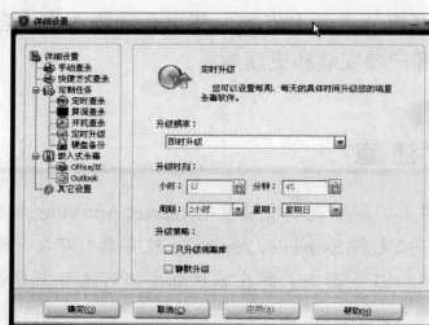
第三层：进程活动行为判定层（危险行为判定、DNA 识别）

进程活动行为判定层自动收集从前两层传上来的进程动作及特征信息，并对其加工判断。无需用户参与，该层可以自动识别出具有有害动作的未知病毒、木马、后门等恶意程序。

2. 即时升级查杀最新病毒

除了主动防御这一重大更新外，瑞星另外一大亮点就是即时升级，即时升级功能比传统的升级方式更加方便，软件会自动检测最新版本、最新病毒库，自动完成整个升级过程。据介绍，瑞星承诺每天提供不少于 3 次的升级内容。即时升级对查杀最新的病毒木马无疑是非常关键的。软件安装完毕后，在设置向导中会提示你设置升级的

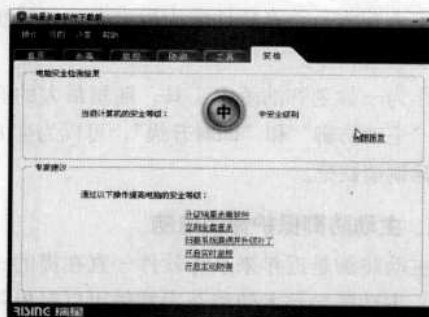
方式，建议大家都选择“即时升级”。也可以点击软件主界面上的“设置”菜单，在打开的窗口中，点击“定时升级”，然后将“升级频率”设置为“即时升级”即可。



定时升级

3. 众多实用工具保安全

瑞星还增加了不少实用功能，以求全力保护系统安全。在软件主界面上，点击“安检”选项，这里软件会自动对系统安全情况进行一个全方位的检测，并提供安全级别标示，同时还提供详细的报告帮助用户修复系统中存在的安全隐患。



系统安全检测

瑞星还提供了账号保险柜的功能，软件安装完毕后，会自动在桌面上建立一个“账号保险箱”的快捷方式，点击即可查看被保护的软件。账号保险柜自动检测用户系统已经安装并被支持的软件。目前支持数量已经达到 104 种。该功能是瑞星中主动防御技术延展出来的应用。账号保险柜可以保护用户的网游、网银等各类软件的账号密码不被木马盗窃。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

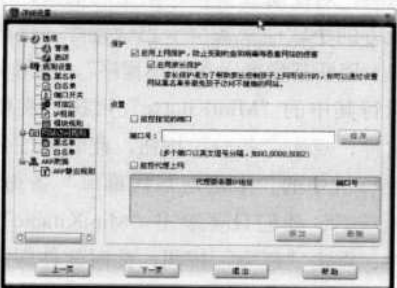
第十三章 局域网安全管理与维护



账号保险柜

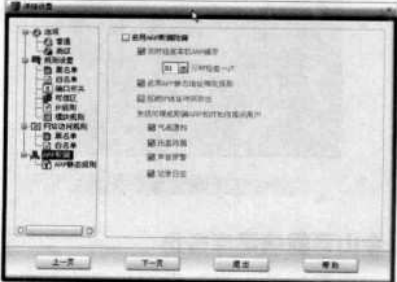
4. 瑞星防火墙功能更强大

除了瑞星杀毒软件的更新外，瑞星防火墙功能也增强了很多，新版提供了家长保护功能，可以帮助家长管理孩子，以防孩子访问不健康网站。具体操作是在点击瑞星防火墙主界面的“设置”选项，然后点击“网站访问控制”选项，这里勾选“启用家长保护”功能。



家长保护

此外防火墙还提供了 ARP 欺骗防御功能，很好地解决了局域网用户深感头疼的 ARP 攻击问题。



ARP 防御

此外，瑞星杀毒软件在资源占用上做了优化处理，比以前版本资源占用更低，界面上也做了

更改，更方便用户的使用，相信“瑞星杀毒软件 + 瑞星防火墙”的组合保护，定能给系统强力保护。

13.3.3 轻松备份杀毒软件病毒库

病毒木马满天飞的今天，装好系统后第一件事情就是安装杀毒软件了，然而安装好后，我们常常遇到“病毒库已过期”的提示，需要大家联网升级病毒库。如果你的电脑没有上网，怎么办？或者你的网速很慢，更新病毒库可能会需要几个小时，等待的过程的是枯燥的，而等待病毒库更新则是提心吊胆的，如果在更新病毒库过程中，自己的电脑中病毒了，怎么办？其实，略施小“技”，就可以在最快的时间完成病毒库的更新，让病毒库随你的系统一起入驻“新家”！

1. 修改注册表转移卡巴斯基病毒库

卡巴斯基在去年和今年的表现一直不错，目前占据了较多的杀毒软件市场份额，下面我们首先来看看卡巴斯基软件病毒库的备份方法。

(1) 备份 / 覆盖卡巴病毒库

一般情况下，卡巴的病毒库放在此文件目录里：C:\Documents and Settings\All Users\Application Data\Kaspersky Lab，将其中的 AVP6（对应卡巴 6.0 版本）或者 AVP7（卡巴 7.0）备份到其他盘。重装系统后，将备份的 AVP 病毒库目录覆盖到新安装的系统对应目录下即可。需要注意：Application Data 文件夹是隐藏的，默认情况下，看不到这个文件夹，依次打开“工具→文件夹选项→查看→隐藏文件和文件夹”，勾选“显示所有文件和文件夹”来进行查看。



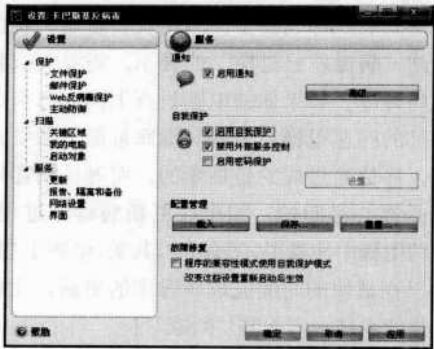
查找病毒库文件夹

注意

文件夹覆盖是有技巧的，由于卡巴斯基软件具有



自我保护功能，因此，必须先关闭其“自我保护”才能进行覆盖。具体操作是：点击任务栏上的卡巴斯基图标，从右键中选择“设置”选项，在打开的窗口中点击“服务”，取消右侧的“启用自我保护”选项即可。

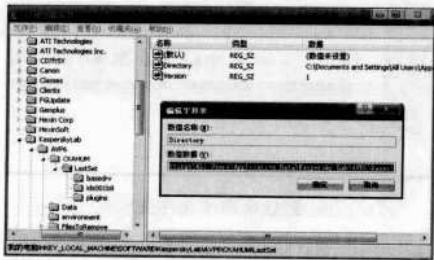


去掉自我保护

(2) 修改注册表转移卡巴病毒库

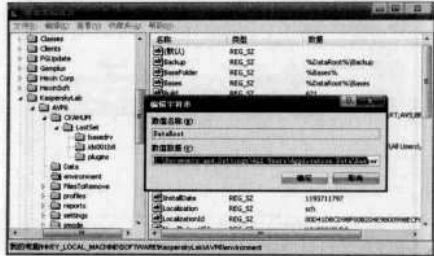
上面介绍的方法可以实现病毒库快速更新，但这种方法不够彻底，如果我们装好系统后，直接将病毒库目录转移到非系统分区，而且让卡巴斯基病毒库更新也保存到新的目录，以后重装系统就不用担心病毒库丢失了。要实现这个目的，我们需要修改注册表，修改相应的保存路径。具体操作如下：

运行“regedit”打开注册表编辑器，依次打开 HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\AVP6\CKAHUM\LastSet，将“Directory”的值修改为新的病毒库保存路径，比如为“G:\AVP”；



修改保存路径

接下来展开“environment”项，将“DataRoot”和“TraceRoot”的值也修改为“G:\AVP”。



更改键值

按照同样的思路，展开“profiles\updater\settings”，将“RetrPath”的值修改为“G:\AVP”。最后展开“profiles\updater\settings\def”，将“RetrPath”的值修改为“G:\AVP”即可。经过以上设置，以后卡巴斯基的病毒库更新会自动保存到“G:\AVP”目录下了。需要提醒大家的是，修改完后，记得开启卡巴斯基的自我保护功能。

(3) 巧用工具备份 / 恢复病毒库

当然，对注册表操作还陌生的朋友，不妨借用第三方的软件来备份卡巴病毒库，这款软件名为“卡巴斯基病毒库备份小程序”，使用非常简单，运行其中的“MiniKit.exe”可执行文件即可打开软件，点击“备份”按钮，此时系统会自动将你计算机中的“卡巴斯基病毒库”备份下来。重装系统后，我们只要双击“MiniKit.exe”可执行文件，点击“还原”按钮，此时软件即完成了还原操作，并提示“病毒库还原完成”。



还原病毒库

2. 金山毒霸病毒库备份

金山毒霸软件本身并没有提供专门的病毒库备份工具，不过我们可以通过“变相升级”的方式来备份和恢复金山独霸病毒库。金山毒霸病毒库保存在安装目录 C:\KAV2009\Update 文件夹中，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十三章 局域网安全管理与维护

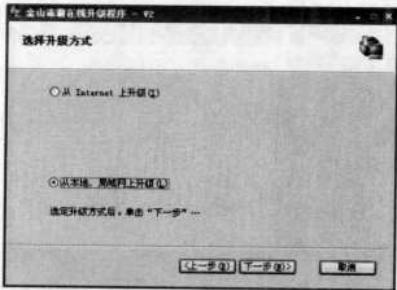
升级的病毒库后都会保存在这个文件夹。



病毒库路径

重装系统之前，可以先将该目录备份到其他分区上，系统重装后，我们就可以利用软件的本地升级功能来“升级”病毒库了，之所以说是变相升级，是因为通常的升级都是从互联网上升级病毒库。具体操作如下：

依次点击“开始→所有程序→金山毒霸 2009 杀毒套装→金山毒霸”，再点击主界面上“工具”选项中的“在线升级”，在打开的窗口选择“自定义升级模式”，点击“下一步”，再选择“从本地、局域网升级”，最后在打开的窗口中选择病毒库备份的路径，按照提示继续即可离线快速升级。



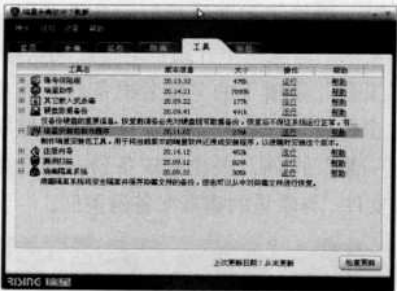
在线升级

3. 瑞星杀毒软件病毒库备份

常用的几款杀毒软件中，瑞星杀毒软件在病毒库备份功能上可以说是最完善的了，瑞星本身提供了制作瑞星安装文件的工具，也就是说，大家可以将自己电脑上包含最新的病毒库的瑞星打包重新制作安装文件，而这个安装文件是可以独立运行的，因此，重装系统后，只要运行你自己DIY的新的安装包即可。因此，在某种意义上说，瑞星不仅仅是备份病毒库，更像是备份整个瑞星

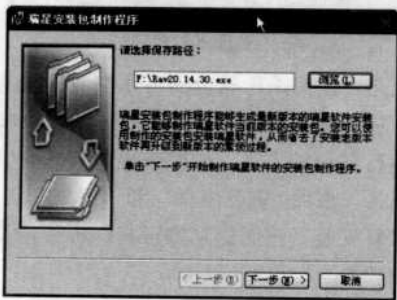
杀毒软件“系统”。

运行瑞星杀毒软件，点击“工具”选项，然后点击“瑞星安装包制作程序”。



工具列表

接下来只要点击其后的“运行”即可开始制作瑞星安装包。在打开的窗口中设置好备份文件的保存路径，默认在系统盘，建议大家更改到非系统分区，这里不多介绍。



制作安装包

接下来按照瑞星的提示进行操作即可。很快，就会弹出一个备份完成的提示。恢复就非常简单了，只需双击这个安装文件运行即可。瑞星杀毒软件这种备份方式不但备份了病毒库，还可以备份你以前在瑞星软件中进行的一系列设置，安装好后，你都可以省去重新设置的步骤了，非常体贴。

如果在瑞星上找不到“制作瑞星安装包”的按钮，可能是由于最开始安装软件时没有安装这个组件。可以通过以下办法来解决：点击“开始→程序→瑞星杀毒软件→添加删除组件”，在弹出的对话框中选择“添加/删除”，点击“下一步”，然后在列表栏中找到“制作瑞星安装包”选项，选中后再点击“下一步”根据提示安装即可。



4. 江民杀毒软件病毒库备份

江民杀毒软件也是大家使用非常多的一款杀毒软件，在备份病毒库方面，江民杀毒软件做得也很体贴，提供了和瑞星类似的备份工具。具体操作不复杂，这里简单介绍：运行江民杀毒软件，点击“工具”菜单下的“重装机备份”选项，在弹出的窗口中，设置好备份文件的保存路径，点击“下一步”按钮，很快完成备份，同样生成一个exe文件，与瑞星的病毒库备份类似。



备份病毒库

但是，江民杀毒软件病毒库恢复方法与瑞星不同，安装好系统后，先安装上 KV2009 软件，然后运行备份的文件，软件将提示你选择安装方式，包括“添加/删除组件”和“修复安装”，选择“修复安装”按照提示即可将病毒库恢复到备份前的版本。

13.3.4 影子系统保护电脑安全

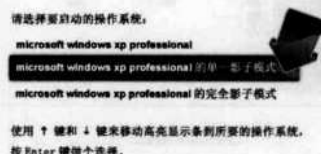
1. 影子系统PowerShadow

PowerShadow 可谓最有名的影子系统了，该软件通过克隆本机硬盘分区，构建现有操作系统的虚拟影像，并形成影子，即影子模式。影子模式和真实的系统完全一样，用户可以进行真实系统的一系列操作，唯一不同的是，进入影子模式后，所有操作都是虚拟的，不会对真正的系统产生影响，一切改变将在退出 Shadow 模式后消失。因此，感觉我们就是“活”在影子中，由于所有操作都是虚拟的，因此，所有的病毒、木马程序、流氓软件都无法侵害真正的操作系统，下面一起来看看。

(1) 影子系统的两种模式

❖ 300 ❖

软件安装完毕后，在操作系统的启动菜单中，我们可以看到增加了两项，分别为对应系统的单一影子模式和完全影子模式，这里可以选择进入正常的操作系统，也可以进入单一影子模式的系统、完全影子模式系统。



启动模式

那么什么是单一影子模式和完全影子模式呢？单一影子模式就是在启动影子系统后，只将你的系统盘作为一个影子，其他逻辑盘不受到任何影响和改变。完全影子模式则是将你的硬盘的所有分区都做成影子模式。因此，他们的区别就在于除了系统盘之外的逻辑盘的操作是否受影响。单一影子模式下，只有系统盘的操作是虚拟的，而完全影子模式下，全部操作都是虚拟的。关于单一影子模式和完全影子模式，可以在“影子系统管理”的“教程”选项中看到直观的图解。



单一影子系统



完全影子系统

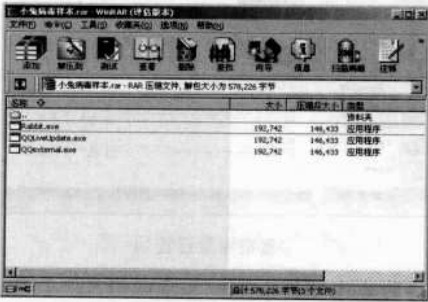
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十三章 局域网安全管理与维护

(2) 影子系统危险操作测试

明白“单一影子模式”和“完全影子模式”的概念后，我们来看看影子系统的实际功能表现，我们以进入“单一影子模式”系统为例，进入系统后，我们可以看到，桌面上的四个角都显示了“单一影子模式”，有点进入“安全模式”的感觉。

进入操作系统后，首先删除了系统盘（C 盘）下的几个文件，重新进入正常的操作系统后，发现完好如初；此外，笔者还安装了几个软件，包括几个广告插件，重新进入操作系统后，也没有发现安装的软件，一切如故；此外，笔者还进行了一项非常危险的操作，那就是直接运行小兔子病毒样本，重启系统后，系统正常运行。看来，影子系统功能确实非同小可。



直接运行病毒，测试系统功能



发现病毒

注意

除了直接重新启动电脑来退出影子模式外，还可以在 PowerShadow 主界面内点击“退出”按钮退出

影子模式。在退出影子模式之前，请确认在影子模式下产生的全部重要数据已经被转移并保存至其他未被保护的物理设备。比如，如果在单一影子模式下，只要保存到非系统分区即可。

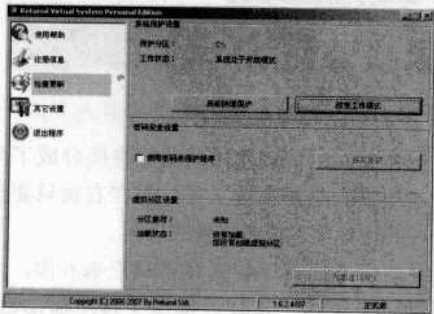


退出影子系统

2. Returnil 虚拟影子系统

前面我们介绍的几个影子类工具，都可以对整个电脑进行保护，而 Returnil 虚拟影子系统 (Returnil Virtual System) 则是通过保护操作系统分区的模式来保护你的系统，该软件是一个基于虚拟机原理的新一代防毒防木马类软件，可以瞬间把你的计算机用隔离罩保护起来，同时用一个内存中的虚假替身：“影子”系统来接管真实的操作系统，因此，其他病毒和木马都无法感染你真实的操作系统。

运行软件后，默认情况下系统处于开放模式，我们可以点击界面中的“改变工作模式”来进行更改，选择“设置系统为保护模式”，设置完毕后，需要重新启动电脑才能生效。



设置工作模式



此外，软件还允许用户设置管理密码，这里不多介绍。设置完毕后，点击“启动快速保护”，将弹出“关闭所有程序”的提示，点击“OK”进入保护模式，进入保护模式后，系统盘的所有操作将不被保存。

Returnil 虚拟影子系统资源占用比较少，最高时只占用 1% 不到的系统资源，而且在空闲时几乎不占用系统任何 CPU 资源。但是该软件功能相对显得比较单一，只能保护系统分区。

13.4 木马查杀与防范

13.4.1 木马防线

木马防线具备间谍软件 / 木马查杀、系统安全管理、实时网络防护等功能。它能够完全查杀国内外流行的 6 万余种木马、后门、蠕虫、间谍软件、广告软件、黑客工具等，它有着优秀的木马查杀引擎，还兼具系统修复等附加功能，能够给你的系统提供全方位的安全保护。

1. 木马查杀傻瓜化

安装完毕后运行该软件，我们首先看到它的主界面如图所示：



程序主界面

主界面左边将该软件的功能主要分成了两大部分：扫描木马和系统工具。而在右侧只要选择要扫描的目标文件或者文件夹即可。

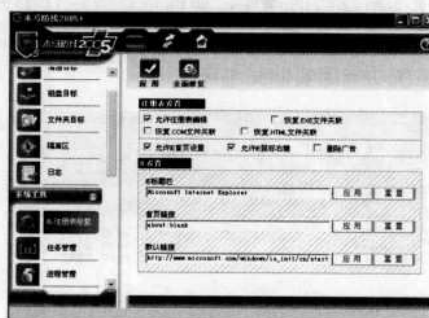
在这个界面可以看到在木马查杀方面，可供选择的选项不少，该软件提供了按照简洁目标、磁盘目标、文件夹目标等查杀条件进行木马的清除。软件还额外提供了敏感区域、内存、光驱等

的扫描，可惜没有比较流行的 U 盘和 MP3 扫描选项，只能从文件夹里进行选择。

2. 系统修复一键搞定

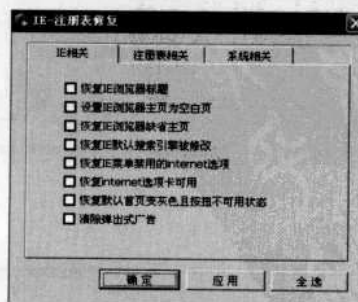
木马防线虽然是一款专业的查杀木马的软件，但是它也有其他附加功能，其中一项就是现在比较流行的 IE 修复了。具体操作如下：

点击“系统工具”下的“IE-注册表修复”选项，这里你可以对注册表进行设置：比如“恢复 .EXE 文件关联”、在注册表被禁用后设置“允许注册表编辑”等，还可以对 IE 的标题栏、默认链接、首页链接等进行设置。



系统修复设置

同时点击该界面上的“全面修复”按钮，你还可以对 IE、注册表、系统三大方面进行相关的设置，涉及到的内容也比较全面，比如“清除弹出式广告”、“恢复注册表被锁”、“恢复阻止用户运行任务管理器”、“恢复隐藏开始菜单中的‘运行’命令”等，基本涵盖了常见的各种问题，相信有了木马防线的帮助，常见的系统修复问题再也不倒你了。

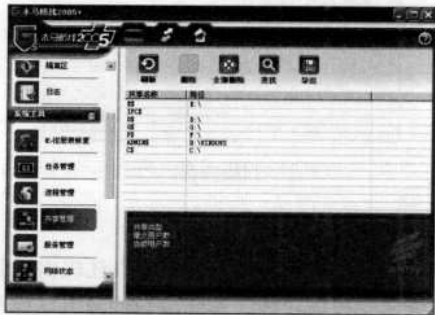


IE 修复选项

第十三章 局域网安全管理与维护

3.共享管理

木马防线还提供了共享管理和任务管理器给我们使用，其中共享管理可以让我们知道电脑里面开了什么文件夹的共享，然后你可以选择进行关闭。值得一提的是，木马防线把系统中的隐性共享文件目录也显示出来了，这让一些对隐性共享不熟悉的朋友多了一份安全感，不要以为自己没有共享文件就安全了，而事实上系统默认有很多东西都是共享的。但木马防线没有提供开启共享的功能。



共享管理

注意

在 Windows 2000 及以后的 Windows XP 和 Windows Server 2003 等操作系统中，系统会根据计算机的配置，自动创建部分特殊共享资源，以便于管理和系统本身使用。尽管在“我的电脑”里这些共享资源是不可见的，在“Windows 资源管理器”也是不可见的，但通过使用共享资源名称的最后一位字符后键入 \$(\$ 也成为资源名称的一部分) 的方法后，别人就能轻易找到这些特殊的共享资源。如果您开机进入系统的密码过于简单，别人就能很快查到您的计算机的地址、用户名及一些简易密码而侵入到您的计算机。这样，这些特殊共享资源就相当于在我们的系统中开了一扇后门，如果不注意防范，危害是非常大的。

4.端口进程管理

通过查看端口的方法可以及时发现一些可疑的病毒、木马程序，从而增强系统的安全。而通过该软件的“端口进程管理”工具，我们可以很

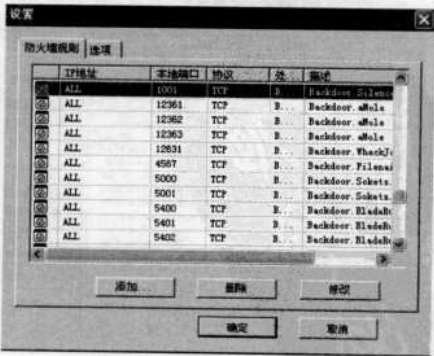
容易就查看到使用的协议、本地 IP 地址、本地端口以及程序路径等，如果端口为 7626，那么我们就可以初步判断是中了“冰河”木马了，这时我们可以点击“终止”按钮来结束该进程，当然这需要我们对端口知识有一定的了解。不过你不熟悉端口也不要紧，只要你的机器能上网，选中进程后，点击右键菜单中的“联机查看进程和端口信息”选项即可连接到安天的网络服务器获取相应的进程和端口信息，十分方便。



端口、进程控制

5.安天盾防火墙

查杀木马后，为了防患于未然，我们应该开启一个木马防火墙，木马防线已经自带一个“安天盾防火墙”，而且它还能够让我们自己设立不同的端口应对不同的防护策略。比如双击 1001 端口，可以在弹出的窗体内选择信任，除了可以指定可信任的外来 IP，还可以指定协议写入自己的相关描述，这个功能非常不错。



安天盾防火墙

此外，木马防线还提供了进程管理、服务管理、

电脑硬道理

点击任何一个选项，在弹出的界面中即可进行相关的检测，比如，我们以“扫描内存”为例，点击该选项后，软件首先会加载病毒库，然后点击“开始扫描”按钮即可进行扫描，很快该软件就给出扫描结果，如果发现木马，则可以点击“清除木马”按钮来进行清除。



扫描内存

2.扫描系统漏洞

除了常规木马检测外,该软件还提供了强大的系统漏洞扫描功能,系统漏洞检测可以检测当前系统可能存在的安全漏洞隐患,并且提供微软官方补丁程序下载地址,使系统安全性大大提升。

点击“扫描系统漏洞”按钮，该软件将自动打开“风云谷漏洞扫描”工具来进行检测，如果检测到系统漏洞，则点击“下一步”，会自动打开你的浏览器，并显示你需要下载的补丁的链接，下载安装后即可对你的系统打上补丁。

3. 探测可疑模块

“探测可疑模块”功能可以找出嵌入到系统程序的可疑 DLL 模块，并查找系统中的所有可疑文件，对可疑文件进行精确定位，而且还能够从注册表中扫描它的加载键值，删除该键值。

点击“探测可疑模块”按钮，软件会提示先关闭其它正在运行的程序，点击“是”即可开始扫描。扫描完毕，软件会罗列出可疑 DLL 文件的路径，点击右键看到四个选项，可以通过“精确定位文件”来直接打开 DLL 文件所在的文件夹，还可以从注册表中查找相关键值，值得一提的是该软件提供了强行删除运行中的 DLL 模块的功能。



程序主界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十三章 局域网安全管理与维护

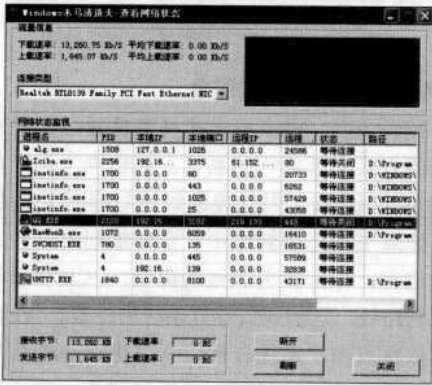


探测可疑模块

4. 监视网络连接

我们知道，木马要窃取被控制的电脑的机密信息，往往需要与远程的主机相连接，因此，看好自己机器的网络连接情况非常重要。

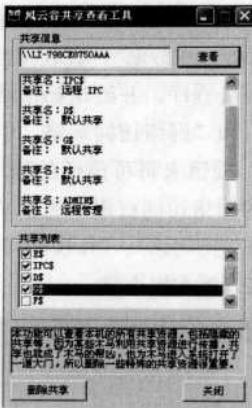
在 Windows 木马清道夫中，点击“查看网络监视”按钮，我们可以轻松查看当前网络的连接情况，这里显示了进程名、本地 IP、本地端口、远程 IP 等网络连接信息，如果我们发现可疑连接，我们可以马上断开网络连接来避免木马的攻击。



查看网络信息

5. 查看共享目录

因为某些木马可能利用共享资源进行传播，共享就为木马进入其他系统打开了一道大门，Windows 木马清道夫提供了“查看共享目录”功能，使用此功能就可以查看本机的所有共享资源，包括隐藏的共享等，从而进行有效的监控。



查看共享

这里，显示了你共享的文件夹以及系统的默认共享，你可以在“共享列表”中勾选上不需要共享的文件夹，然后点击下方的“删除共享”按钮即可。

除了以上几个功能外，Windows 木马清道夫还具有“清理内存”功能，可以释放内存空间，使系统开机加速。还可以利用该软件备份注册表，如系统有异常情况，可以随时进行注册表恢复。

Windows 木马清道夫是一款适合于所有网络用户的安全软件，既有新手使用的扫描内存、扫描硬盘、扫描注册表、清理内存等傻瓜按钮，也有可供高手使用的进程管理，模块信息管理等强大功能。它提供了专业的分析功能，完美的升级功能，让你不再惧怕木马，从此远离木马的困扰！

13.4.3 微点主动防御软件

“微点主动防御软件”能自动准确判定新病毒，在全面监视程序运行的同时，自主分析程序行为，发现新病毒后，自动阻止病毒行为并终止病毒程序运行，自动清除病毒，并自动修复注册表，还能自动提取特征值实现多重防护，下面就一起来看看这款强大的系统保护工具。

1. 安全防护，“多”管齐下

安装完毕后运行该软件，从软件的主界面即可看到该软件的几大功能：安全防护与策略、系统分析、网络分析、安全日志、系统日志等。在安全防护与策略中，该软件提供了可疑程序诊断、



漏洞扫描、有害程序隔离等多达 6 类的安全保护。

点击“可疑程序诊断”，该软件会自动检测当前进程中的可疑程序，并给出扫描结果。在“修改程序策略”和“网络访问策略”中，我们可以点击“添加”按钮来将可信任的程序添加进来，并设置适当的网络访问权限，包括“允许访问网络”、“不允许访问网络”、“每次询问”，这跟普通防火墙的规则设置大同小异。



添加可信任程序

2.漏洞扫描，消除隐患

在“安全防护与策略”中，非常值得一提的就是该软件强大的“漏洞扫描”功能，大家都知道漏洞对于系统的安全是非常致命的威胁，然而对新手而言，系统存在哪些漏洞，如何下载、安装补丁，这是他们感到非常烦恼的问题。用微点主动防御软件，这个问题就轻松搞定了。

点击“漏洞扫描”选项，经过一段时间的扫描后，在软件界面右侧将会列出当前系统中存在的漏洞，而且还有相关的漏洞说明，点击后面的“下载补丁”链接即可下载并安装相应的补丁。怎么样，你还为系统漏洞补丁担心吗？



漏洞扫描

3.巧妙设置，自动防护

前面给大家介绍了微点主动防御软件的几个非常强大的功能，那么能否让该软件具有杀毒软件那样的自动监控、自动防护功能呢？答案是肯定的，要让软件自动防范各种病毒等有害程序，我们需要先进行简单的设置，点击主界面上的“安全防护与策略”，再次点击“程序行为实时监控策略”，在右侧的设置界面中勾选“自动处理”或者“询问后处理”，这个类似于通常的杀毒软件的功能。为防止软件误删除文件，我们最后选择“询问后处理”，设置完后后，点击“保存”按钮即可自动防护有害程序了。



自动防护

4.控制进程，确保安全

我们知道，很多病毒木马都是通过入驻系统进程的方式来破坏你的系统，如病毒木马经常利用的 svchost.exe，因此控制好进程是很关键的一环。微点主动防御软件中，会详细列出当前系统中的进程，并有相关进程的说明，以及在系统中运行的路径，这为我们看好系统进程很有帮助。

依次点击“系统分析”→“进程综合信息”，这里将进程分成了 Windows 系统进程、其他软件进程、应用软件进程三大类，点击“Windows 系统”进程，点击任意一进程，将会在右下侧显示进程的模块名称、分类、程序说明以及全路径。通过这个，我们就可以看到该进程调用的所有 DLL 文件，有的木马就混杂在这里，如何识别哪些是木马呢？其实很简单，因为该软件将非系统调用的 DLL 文件都以蓝色高亮显示，这样，你就可以根

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第十三章 局域网安全管理与维护

据该软件提供的“全路径”找出这些木马，然后进入安全模式删除该文件，即可手动清除木马了。



清除木马



注意

在“系统自启动信息”中，我们还可以查看当前随系统一起启动的文件，可能木马就潜藏其中哟！在“注册表修复”中，还能进行 IE、任务管理器、注册表锁定等注册表修复工作。

5.未知木马，照样截杀

除了以上介绍的几大功能外，微点主动防御软件最有特色的地方还在于能够截杀未知的木马、病毒，这在网络病毒频发的今天非常有用。在新病毒被杀毒软件厂商截获，并给出解决方案前，可能很多病毒木马已经入侵很多用户的系统了。

笔者为此专门做了一个试验，在机器上安装了一个黑客工具，再次运行微点主动防御软件时，马上弹出提示框，发现未知木马：

这里提示你是否上报给该软件厂商，从而添加到该软件的病毒库中，为了截杀更多的木马，我们最好选择上报。

与此同时，我们在有害程序中发现了上面截获的未知木马。依次打开“安全与防护策略”→“有害程序隔离”，这里我们可以看到“删除时间”以及“原始文件”的路径，知道了文件路径，要清除该木马就非常简单的了。同时我们也可以利用软件提供的删除功能来直接删除。



删除木马

6.日志管理，了然于心

微点主动防御软件还提供了非常强大的日志管理功能，包括“安全日志”和“系统日志”两大类，其中安全日志里面有病毒日志、木马日志、溢出日志、蠕虫日志、网络入侵日志等，里面详细记录了时间、进程名、处理结果等。强大的日志管理功能，可以让你随时掌控自己电脑的安全。



注意

在软件主截面上方，还提供了系统当前的实时网络连接情况，包括当前连接数、远端地址、进程数等，其中远端地址中显示了 IP 地址，并注明了所在的地区，这非常方便你查看是否恶意的连接。

微点主动防御软件是一个功能非常强大的软件，从系统到网络提供了全方位的安全保护，其独特的未知病毒查杀功能，更加有效地增强了对系统的保护功能，实在是一款不可多得的安全工具。

13.5 用户数据的安全备份

13.5.1 系统自带备份与还原工具

数据的备份与还原在网络安全中可谓是一件重中之重的操作，它是绝不可忽略的！试想，在黑客让你的数据完全“消失”后，你却可以在数分钟内通过备份文件让一切重现，这种失而复得

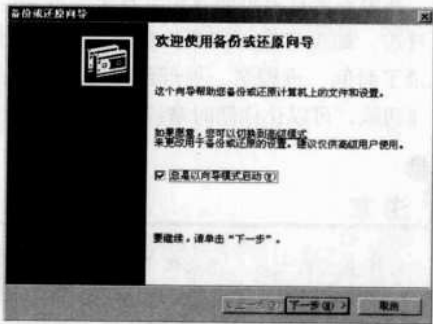


得的感觉不是笔墨可以形容得出的哟！下面就以 Windows Server 2003 的“备份与还原向导”为例讲述一下数据的备份与还原方法！

1. 备份数据

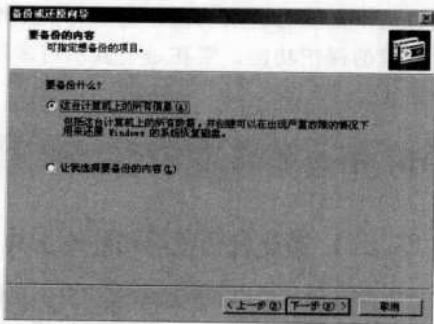
“备份与还原向导”是 Windows 2000/XP/2003 中内置的组件，它的功能极其强大——它既可以备份系统的所有数据，也可以备份用户指定的数据，使用它可以极好地完成系统中各种数据的备份与还原应用。使用它备份数据的过程如下：

依次点击“开始”→“程序”→“附件”→“系统工具”→“备份”菜单项，启动“备份或还原向导”。在欢迎界面中选择默认状态后，点击“下一步”按钮继续。



备份向导

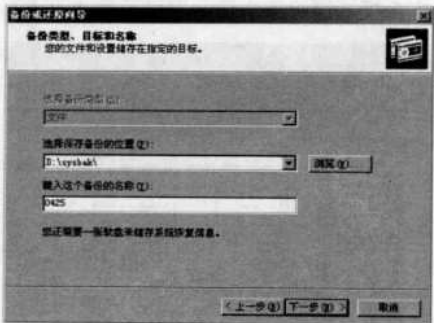
接下来选择“备份文件和设置”项后继续。在“要备份的内容”对话框中，选择“这台计算机上的所有信息”项后继续。



选择备份内容

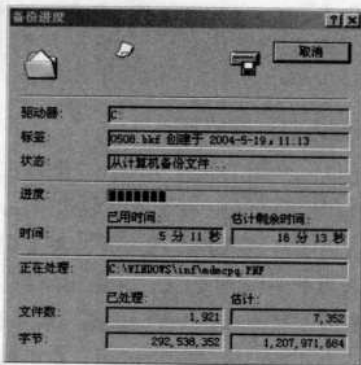
“备份类型、目标和名称”对话框中，基于安全考虑，请在使用 NTFS 文件系统的分区设置一个目录（如 sysbak）用于存储备份的数据，在“名

称”项中可以键入备份日期等易于管理的名称。



输入备份文件信息

设置完毕后，就可以在下一步的对话框中直接点击“完成”按钮继续了。稍后备份向导将自动开始指定数据的备份操作，因上述操作中已指定备份所有的数据，所以备份向导会需要很多的内存来支持，此时请将一些暂时不用的应用程序关闭以节约内存。



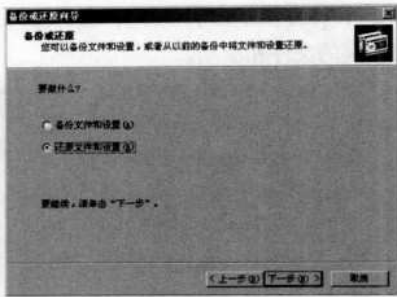
备份过程

最后，备份向导将会弹出一个提示框，要求插入一张空白的、容量为 1.44MB 的已格式软盘，从提示信息中可以看出恢复信息（即 Sar.sif 和 Sarpnp.sif 及 Setup.log 这三个文件）将会被写入这个软盘。在软盘制作完毕后，我们可以看到备份文件已经创建成功了。此时点击“确定”按钮即可结束备份操作。

2. 还原数据

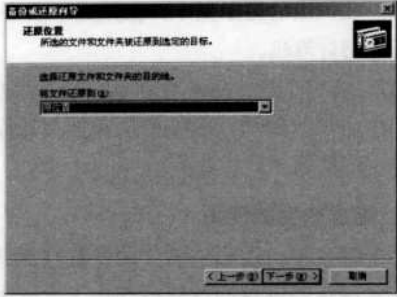
当系统出现故障需要还原数据时，请在能够进入系统的情况下，运行“备份或还原向导”。首先要选择“还原文件和设置”项后继续。

第十三章 局域网安全管理与维护



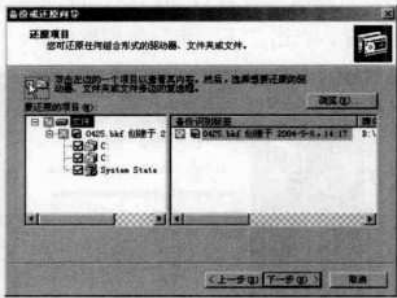
选择还原

在“还原项目”对话框中找到以前备份的文件“0425.bkf”，并在左窗中将要还原的项前打上勾后继续。



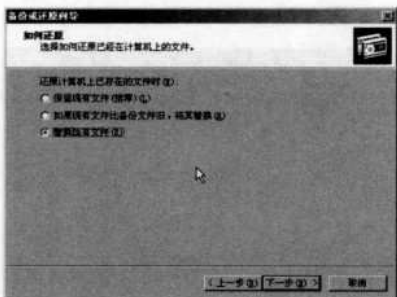
设定还原位置

在“如何还原”对话框中选择“替换现有文件”项继续。



勾选还原文件

设置完毕后，在下一步界面中点击“完成”按钮结束设置。

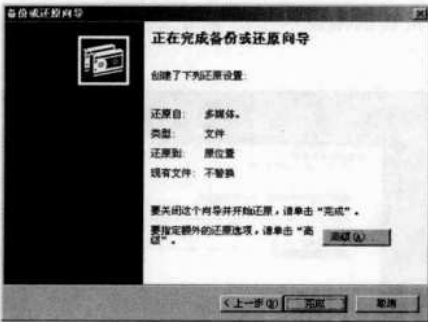


替换文件

在“高级还原选项”一步中请选择“还原安全设置”、“还原交接点”，但不还原交接点引用的文件夹和文件数据”、“保留现有卷的装入点”项后继续。

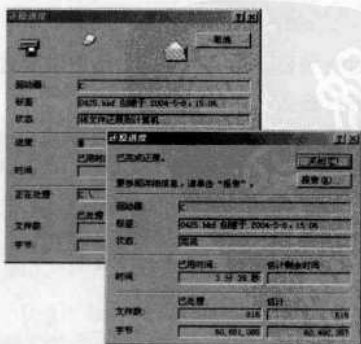
设置完毕后，在最后的界面中将会看到“现有文件”项改换成“总是替换”状态了。此时请点击“完成”按钮继续。

稍后请耐心等待还原过程的结束。



完成还原设置

请注意，因为在恢复时如果对现有文件不替换，很容易出现因磁盘空间不足而导致恢复失败的情况，并发的后果则可能是导致启动失败。所以此时应点击上图中的“高级”按钮，在进入“还原位置”对话框时，请将“将文件还原到”项设置为“原位置”项。



还原过程



最后在弹出的提示框中，根据提示点击“是”按钮后重启计算机。

通过上述的备份与还原操作，我们就可以在 Windows 出现故障后，轻松使用备份与还原功能来将系统恢复到完好状态了。

3. 恢复软盘的使用

再来看看备份过程中制作的恢复软盘使用方法，这张磁盘当硬盘出现故障并丢失所有配置参数和信息时就可以使用到它了。它的使用方法是：

首先使用 Windows 系统安装光引导系统并进入安装程序，在出现文本安装模式时根据下方的提示按 F2 键。



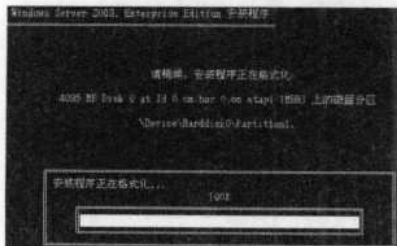
进入安装程序

下一步中根据提示插入 ASR 恢复软盘。



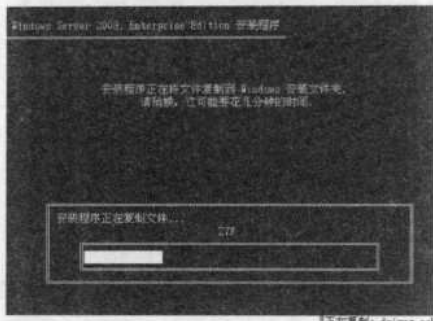
插入软盘

稍后安装程序会自动启动 ASR 恢复过程，它首先会进行磁盘分区的格式化操作。



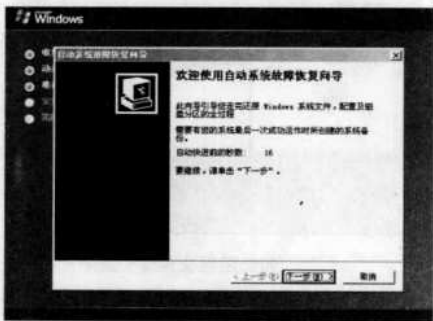
恢复参数

接下来安装程序会安装一个最小化的系统，并安装必要的文件和驱动。



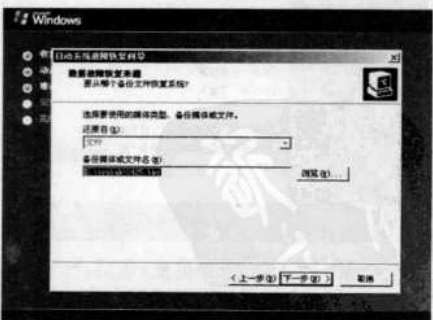
安装必要文件和驱动

安装完成后系统会自动启动“自动系统故障恢复”向导，点击“下一步”按钮继续。



启动自动恢复

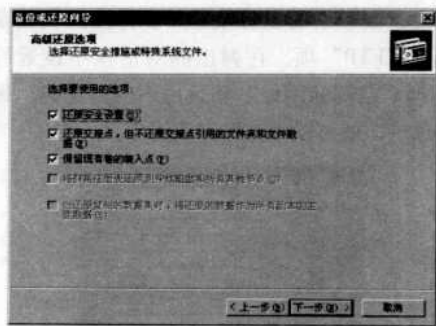
接着根据提示指出备份文件的路径和文件名后继续。



输入备份文件信息

下一步中点击“完成”按钮即可开始数据的恢复，在耐心等待数据恢复完成后重新启动计算机即可。

第十三章 局域网安全管理与维护



完成后重启计算机

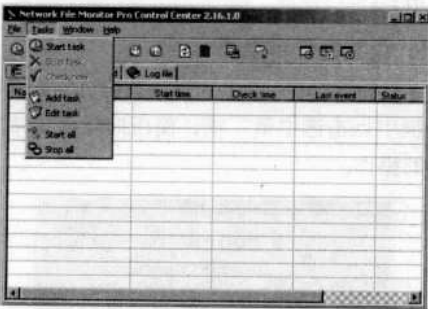
看，备份与还原的操作并不复杂，但却可以很好地保障我们的系统安全。这样的功能怎能不好好地学习一下呢？当然，学会后还要将其真正地应用到实际操作中才行，这样才能更好地掌握好知识。

13.5.2 同步网络文件

为了安全起见，我们要做好重要文件的备份操作。为了让网管人员从繁重的备份操作中解脱出来，我们不妨使用 Network File Monitor Pro 来完成特定文件的同步备份操作。

1. 设置备份目录

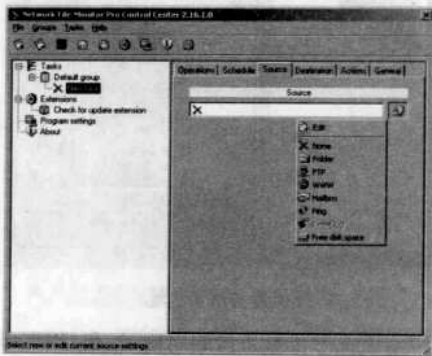
在进入程序主窗口后请点击“Tasks”下的“Add task”菜单项，新建一个任务。



新建任务

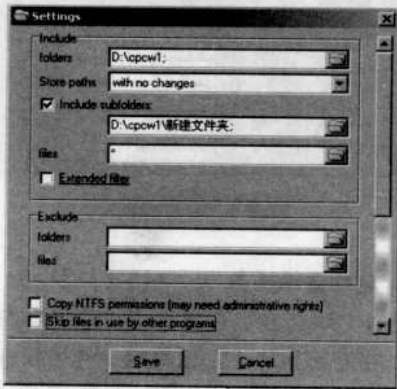
在接着弹出的窗口中可以看到“Tasks”项的“Default group”下已经有了一个“Add task”，这表明已经新建一个任务了，下面让我们先来对其进行设置。首先点击“Source”选项

卡设置面板中的设置按钮，在弹出的快捷菜单中选择“Edit”项。



编辑任务信息

在弹出的对话框中，首先选中要备份的来源主目录（如 D:\cpcw1），如果想让主目录下的目录也进行备份，接着点击勾选“Include subfolders”项，然后点击右侧的按钮，在弹出的对话框中添加子目录。在“files”项中输入“*”（即所有文件）。



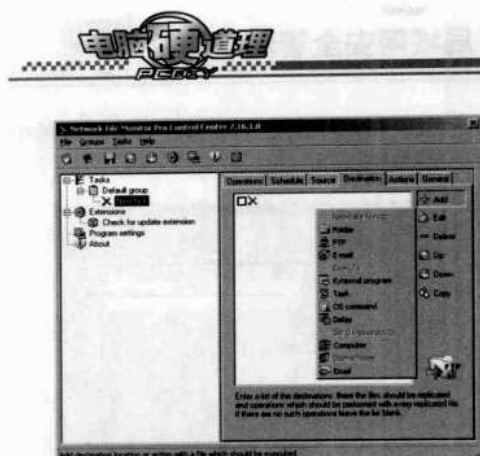
添加备份来源



注意

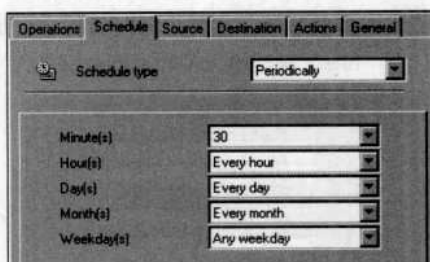
这里还可以通过“Exclude”项中设置一些不进行备份的目录和文件。

接着在“Destination”选项卡设置面板中点击“Add”按钮，在弹出的快捷菜单中选择“Folder”项，添加目的地目录即可（如 cpcw 目录）。



设置备份目的地

接着就需要设置备份的周期了，在“Schedule”选项卡设置界面中这里将“Schedule type”项设置为“Periodically”；将“Minute”项设置为了“30”。下面的默认项。这个设置的效果是每小时的 30 分时自动备份一次。



设置自动备份时间

2. 启动备份任务

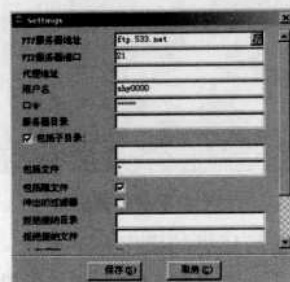
设置完毕后我们还需要手工启动备份任务才行，在返回到程序主窗口后，选中任务列表框中的任务，然后点击“Tasks”下的“Start Task”菜单项，随即选中的任务将自动开始备份一次，然后才会按指定时间自动进行备份和相应操作。

3. 同步FTP服务器

如是你有两个 FTP 服务器空间，那么在第一个 FTP 服务器上上传好所有文件后，就可以使用 Network File Monitor Pro 来完成两个 FTP 服务器空间的内容同步，这样就可以让我们不必再一次进行第二个 FTP 服务器的内容上传操作了。

首先新建一个任务，然后点击“Source”选

项卡设置面板中的设置按钮，在弹出的快捷菜单中选择“FTP”项。在弹出的对话框中设置好第一个 FTP 空间的网址、登录用户名和密码、端口等信息后，就可以将其保存设置了。



设置FTP信息

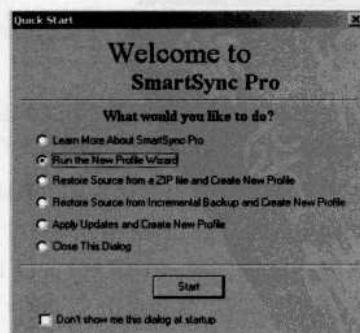
接着在“Destination”选项卡设置面板中点击“Add”按钮，在弹出的快捷菜单中选择“FTP”项，在弹出的对话框中添加目的地 FTP 服务器信息即可。在设置完毕并启动任务后就可以在指定的时间里自动同步两个 FTP 空间的内容了。

13.5.3 网络备份

SmartSync Pro 是一个专业的数据备份软件，它可以非常好地完成各种基本的数据备份工作，同时它也支持网络备份，显然这将给局域网环境中的备份带来莫大的方便。下面让我们来看看怎样使用它。

1. 设置备份目录源

在运行 SmartSync Pro 后，我们可以在弹出的对话框中点击选中第二项，使用向导模式来完成备份的操作。

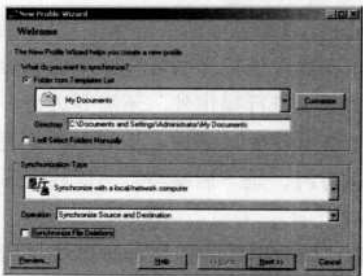


备份向导

第十三章 局域网安全管理与维护

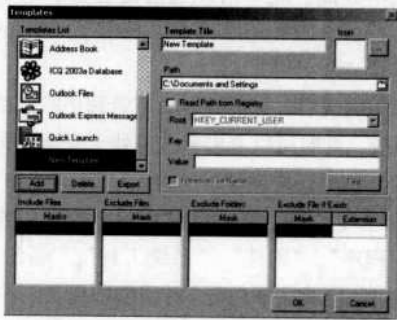
Chapter

在弹出的对话框中我们即可在“Folder from Templates list”项中选择列表中的备份源进行备份。



选择备份源

也可以通过点击“Customize”按钮，在弹出的点击“Add”按钮，在“Template Title”中设置标题，在“Path”项中设置新建任务的源路径。

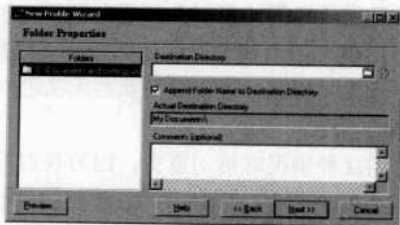


创建备份任务

设置完毕后点击“OK”按钮返回上一步界面后，我们就可以开始设置备份文件的目的地了。

2. 设置备份目标目录

我们既可以在“Synchronization Type”项中选择远程计算机项，也可以选择“Synchronize with a local/network computer”项继续。接着在下一步中点击“Destination Directory”项右侧的“目录”图标。



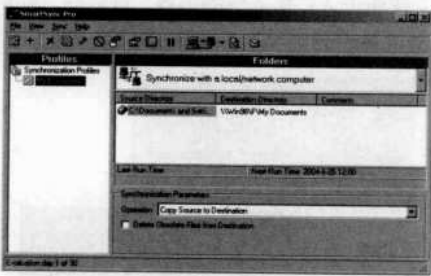
选择备份目录

接着弹出的选择对话框中点击“网上邻居”，从中选择局域网中准备用作备份目标的计算机，然后展开其下的共享目录，选择好准备用于备份数据的目录后点击“确定”按钮继续。



目标计算机必须先设置好共享目录，才能在设置时看到。

随后弹出的提示对话框中点击“yes”按钮继续，再根据具体情况设置好时间与频率。接着为新建的备份操作起个任务名即可完成设置。在返回到主界面后可以看到新建的备份操作已经在列表中了。



查看备份列表

此时既可以按 F5 键立即开始备份操作，也可以任由程序在指定的时间自动进行备份操作了。

13.5.4 服务器数据库的备份与还原

作为集中管理网络资源、提高用户访问资源效率的重要服务，AD（Active Directory，“目录服务”）的重要性对每一位网管来说都不言而喻！网络安全中，如果数据库被黑客攻击，损失必将不可估量，为了让数据库也可以安枕无忧，下面就让我们一起来学习 AD 数据库的备份与还原吧！

1. 为什么要备份

将 AD 数据库进行备份，是基于数据库中庞大的数据量而言的，假设一家大型企业的 AD 数据库中有上千名用户数据，如果 AD 数据库遭到黑客们有意或无意的损害，导致了用户数据的丢失，此时如果逐笔恢复数据，那么工作量无疑将



是惊人而漫长的！所以，有经验的网管们通常会定期进行 AD 数据库的备份，当 AD 数据库出现种种问题时，就可轻松完成 AD 数据库的数据还原，而很多网管却对这么重要的备份操作并不了解或忽视！

2. 备份AD数据库

备份 AD 数据库的操作并不复杂，因为备份操作是通过备份向导来完成的，所以即使是菜鸟级网管也可以轻松上手。过程如下：

依次点击“开始”、“程序”、“附件”、“系统工具”、“备份”，在打开的“备份或还原向导”对话框中点击“下一步”按钮进入“备份或还原”选择对话框。

在选择“备份文件和设置”项后，点击“下一步”按钮进入“要备份的内容”对话框，选择“让我选择要备份的内容”项并点击“下一步”按钮。



备份数据库

在“要备份的项目”对话框中依次展开“桌面”、“我的电脑”，点击勾选“System State”项。

在下一步的“备份类型、目标和名称”对话框中根据提示选择好备份文件的存储路径，并设置好备份文件的名称后，按“下一步”按钮。接着在打开的对话框中点击“完成”按钮。

此时请中断计算机中的其它操作，因为片刻后 AD 数据库的备份操作就会开始进行了。

在备份过程中，有可能会跳过一些文件进行备份，这种情况并非是备份的 AD 数据库不完整，不必担心。

如果想知晓哪些文件被跳过，可以在备份完

成后弹出的对话框中点击“报告”按钮查看。

3. 还原AD数据库

相对于 AD 数据库的备份操作，AD 数据库的还原操作就显得稍微有些复杂了。因为除了按备份向导的提示进行操作外，还需要进行一些额外的操作才能顺序完成还原，主要的原因是 AD 服务正常运行时，是不能够进行 AD 数据库还原操作的。

所以 AD 数据库的还原操作应按进行如下方式进行：

(1) 进入目录服务还原模式

在重新启动计算机并进入 Windows Server 2003 的初始画面前，按 F8 键进入 Windows 高级选项菜单界面。此时可以通过键盘上的上下方向键选择“目录服务还原模式（只用于 Windows 域控制器）”项。

回车确认后，将需要以具有管理员权限的账户登录系统，此时可以看出系统是处于安全模式的。

(2) 使用还原向导

在进入目录服务还原模式后，依次点击“开始”、“程序”、“附件”、“系统工具”、“备份”，在打开的“备份或还原向导”对话框中点击“下一步”按钮继续进入“备份或还原”选择对话框，选择“还原文件和设置”项。接着在进入下一步的“还原项目”对话框后，依次展开并选中备份文件。

在稍后弹出的界面中点击“完成”按钮。稍待片刻后，系统将弹出一个警告提示框，点击“确定”按钮，确认数据库的覆盖操作可以开始。稍后系统将自动开始 AD 数据库的还原操作。

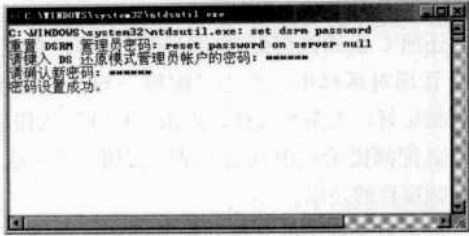
完成还原操作后，点击对话框中的“关闭”按钮就可以结束了。最后将会弹出一个“备份工具”提示框，点击“是”按钮重新启动计算机即可。

最后需要提醒的是，有些朋友还原 AD 数据库时会出现忘记当初设置的还原密码（添加 AD 服务时设置）情况，这个时候就会无法进入目录还原模式了。

遇到这种情况时请勿慌张，因为我们可以通过依次点击“开始”、“运行”，在弹出的运行栏中输入“Ntdsutil”命令的方法，在弹出的窗口中进

第十三章 局域网安全管理与维护

行进入目录还原模式密码的重设操作。



重设还原密码

上图中“Set dsrm Password”命令用于修改任意域控制器的“Active Directory 恢复模式”管理员口令。而“Reset password on server null”命令则是用于“直接在进行目录还原的计算机上重新设置还原密码时”使用的。

设置还原密码成功后，还需要重新启动计算机，重启后即可使用新的还原密码进入目录服务还原模式了。

13.5.5 Windows服务备份

在局域网环境中，网管往往非常重视对 Windows 服务器硬盘中的用户数据文件的备份，而忽视了对 Windows 系统本身提供的各种服务的状态信息和服务数据的备份，如 IIS 服务、DHCP 服务、DNS 服务等，这些 Windows 服务在局域网中往往起着非常重要的作用，如使用 IIS 架设企业内部网站，使用 DHCP 服务为局域网用户统一分配 TCP/IP 配置信息等，一旦这些服务出现问题，就会严重影响用户的正常办公。

因此网管也要重视对 Windows 服务的备份，一旦某些 Windows 服务出现问题，可以立即使用备份的文件进行恢复，真正做到有备无患。

对 Windows 服务的备份一般要分成两部分进行备份：状态信息备份和数据备份。

Windows 服务的状态信息备份需要通过手工备份注册表相应的项目来完成，一般是一次可以备份全部的 Windows 服务状态信息；而服务数据的备份，则需要单独进行，可以使用手工方式、服务自身提供的工具或者使用第三方软件来完成。

1. 备份服务状态信息

各种 Windows 服务的状态信息一般都是存储在注册表的“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”项目下，网管可以通过备份该项目，来完成对 Windows 服务的状态信息的备份。

在 Windows 服务器提供的各种服务正常运行状态下，点击“开始→运行”，在运行对话框中输入“regedit”命令后回车，在注册表编辑器对话框中依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”项目。

各种 Windows 服务的状态信息就存储在“Services”项目中，网管只要将此项目的内容备份出来即可。备份操作非常简单，在注册表编辑器中选中“Services”项目，然后点击主菜单栏中的“文件→导出”选项，弹出“导出注册表文件”对话框，为该备份文件起个名字，指定好存放路径后，最后点击“保存”按钮，完成 Windows 服务状态信息的备份。

当某些服务的状态信息出现问题时，只要双击该备份文件，将备份的状态信息重新导入注册表即可。

对于服务数据信息的备份，网管则要单独进行备份操作，一次只能完成一种 Windows 服务数据信息的备份。对于 Windows 系统提供的如此多的服务类型，这里将以 IIS 服务、DHCP 服务以及磁盘配额等为例，介绍如何单独对它们的数据信息进行备份。

2. IIS服务备份

IIS 服务器中内置了备份和还原工具，利用该功能可以快速地完成本地 IIS 服务器数据信息的备份和还原工作。

在“Internet 信息服务”控制台窗口中，右键点击 IIS 服务器，选择“所有任务→备份/还原配置”选项，然后在“配置备份/还原”对话框中点击“创建备份”按钮，接着在“配置备份”对话框中为备份文件起个名字，如果要对备份文件进行加密，可以启用文件加密功能，这时要选中“使用密码加密备份”选项，接着输入文件加密密码，最后



点击“确定”按钮，就完成了 IIS 数据信息的备份操作。

当 IIS 服务器由于数据信息损害而出现问题，需要还原 IIS 数据信息的时候。

在“Internet 信息服务”控制台窗口中，右键点击 IIS 服务器，选择“所有任务一备份/还原配置”，在“配置备份/还原”对话框中选中你需要的备份文件，然后点击“还原”按钮，如果备份文件被加密，则需要输入密码，即可完成 IIS 数据信息的还原。此外对 IIS 服务器数据信息的备份还可以使用第三方软件，如 IIS 备份精灵、IIS Export Utility 等，这里就不再赘述了。

3. DHCP 服务备份

DHCP 服务器也内置了备份和还原功能，并且操作同样简单。在 DHCP 控制台窗口中，右键点击“DHCP 服务器名”选项，在弹出的菜单中选择“备份”，然后在“浏览文件夹”对话框中指定好备份文件存放的路径，点击“确定”按钮后，就完成 DHCP 服务器的数据信息的备份。

一旦 DHCP 数据信息被损坏，需要进行恢复时，再次右键点击“DHCP 服务器名”选项，在弹出菜单中选择“还原”，然后指定好备份文件所在的路径，点击“确定”按钮后，Windows 系统会停止 DHCP 服务，然后再重新启动该服务，就可以完成 DHCP 数据信息的还原。

4. 磁盘配额备份

网管为了增强服务器的安全性，使用 Windows 系统提供的磁盘配额功能，对每个用户使用的服务器磁盘容量进行限制。但如果服务器由于某些原因，网管配置的这些磁盘配额项目丢失了，手工恢复是非常麻烦，因此网管也要提前备份好这些磁盘配额项目。

备份磁盘配额项目非常简单，这里以备份 Windows Server 的 C 盘的磁盘配额项目为例，右键点击“C 盘”盘符，在弹出的菜单中选择“属性”选项，接着切换到“配额”标签页，然后点击下方的“配额项”按钮，弹出“配额项目”管理对话框，点击“配额一导出”，在“文件名”栏中为备份文件起个名字，最后点击“保存”按钮，完

成磁盘配额项目的备份。其它盘符的磁盘配额项目备份同上面相同，不再赘述。

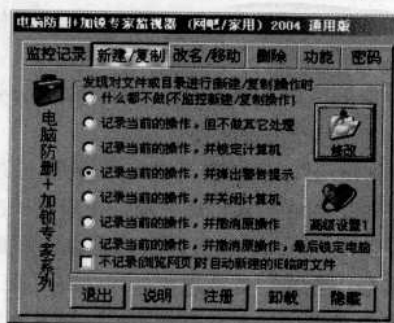
还原 C 盘的磁盘配额项目同样简单，在配额项目管理对话框中，点击“配额一导入”选项，接着指定好以上备份文件，点击“打开”按钮后，在磁盘配额提示框中点击“是”按钮，就完成磁盘配额项目的还原。

以上只是简单的介绍几种 Windows 服务的数据信息的备份和还原，其它种类的 Windows 服务数据信息的备份和还原操作也非常简单，大家可以在日常的维护工作中慢慢体会和实践。

13.5.6 用电脑防删专家保护文件

虽然现在的计算机发展迅速，但还没达到每人一台的地步，特别是企事业单位里的计算机，大都是公用计算机，在这种情况下如何保护自己的文件不被别人误删除便成为摆在这些用户面前急待解决的问题了。

各种类型的数据文件是我们保存在计算机上的巨大财富，但病毒、误操作和存储介质故障等不可预知的潜在危险时刻都在威胁着我们的重要数据文件的安全。因此，灾难数据恢复工具是 IT 人员的必备工具。“电脑防删专家”采用最新 Vxd 技术与 Windows 内核句柄相结合的监控方式，监视电脑中的新建、重命名、移动、复制、删除文件或目录。也可以将改变文件关联、添加、删除网络共享等操作记录下来以供查阅。可以设定多种防删除、防复制、防新建、防改名、防移动等管理方案，有效地保护用户自己的文件。



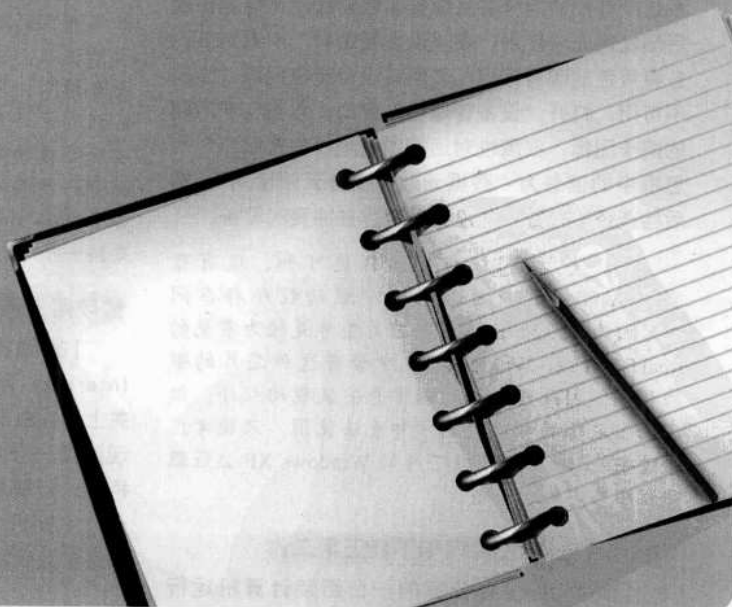
电脑防删专家

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

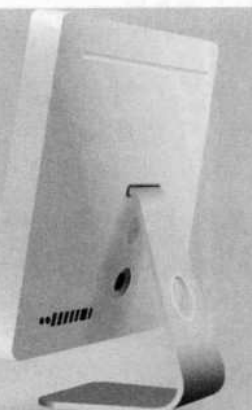
故障解决篇

第十四章 局域网故障排除实例

- 网卡、网线故障排除实例
- 路由器、交换机故障排除实例
- 网络连接故障排除实例
- 网络设置故障排除实例
- 网络权限设置故障排除实例
- 其他网络配置故障排除实例



第十四章 局域网故障排除实例



网络设备及其基本连接、配置是网络组建的基础，这其中主要涉及到路由器、交换机、网卡、网线、网络协议配置、网络权限设置等方面，在网络管理过程中，如何高效地维护这些设备，并对出现的故障及时进行处理是网管们非常关心的问题，本章将以一些实例来进行分析，并给出行之有效的解决方法。

14.1 网卡、网线故障排除实例

TP-LINK网卡无法正确安装

【故障现象】一台局域网计算机运行 Windows XP 操作系统，现在想为其安装一块型号为 TF3239D 的 TP-LINK 网卡。安装后启动 Windows XP 系统，系统能够找到网卡并且能安装驱动程序。但是安装后却发现无法使用，在“设备管理器”中看到该设备有黄色的叹号标识，表明该设备存在问题，当前不可用。打开“设备管理器”窗口，双击存在问题的网卡图标，在属性对话框中看到“设备状态”信息框中的信息为“数据无效，设备无法使用”。然后检查资源设置，并没有发现存在冲突的设备。

【解决方法】根据故障描述可知，很有可能是 Windows XP 自带的网卡驱动程序存在问题。因为 TF3239D 网卡的芯片型号是较为常见的 RealTek8139，Windows XP 中含有这种芯片的驱动程序，因此可以识别网卡并安装驱动程序。但已经安装驱动程序的网卡却无法使用，只能考虑通过安装 RealTek8139 芯片的 Windows XP 公版驱动程序来解决此问题。

RealTek 8139芯片网卡不能正常工作

【故障现象】办公室的一台组装计算机运行

Windows 2000 系统，网卡（RealTek8139 芯片）能够正常安装且在设备管理器中显示正常状态。在系统托盘中显示出“本地连接”已经连接上，各项网络参数设置正确，可是无法跟局域网中的其它计算机通信。将该网卡安装到其它计算机上，则在设备管理器中显示黄色叹号。应该如何解决？

【解决方法】首先尝试更新网卡的驱动程序，如果网卡的驱动程序有问题，会出现各种各样的奇怪现象，建议更新网卡的驱动程序。如果故障没有排除，接着尝试更换网卡。既然将该网卡安装到其它计算机时会标识有感叹号，则表示存在硬件资源冲突或设备无法正常工作。因此网卡可能有存在问题。如果故障依旧，最后尝试先从设备管理器中删除现有网卡，关闭计算机后为网卡更换一个 PCI 插槽并重新安装驱动程序。

修改网卡速率突破100米限制上网

【故障现象】某学校通过教育城域网接入 Internet，所有的计算机均使用固定 IP 地址经网关上网。由于临时需要，同时也本着做实验的目的，现通过一条约 120 米的网线连接一台计算机和交换机。计算机上安装的是 10M/100M 自适应以太网卡，交换机也支持 10M/100M 自适应。设置好各项网络参数后发现计算机可以上 QQ，但不能浏览网页。

第十四章 局域网故障排除实例

可以排除 DNS、病毒、网络设置等方面的原因。

【解决方法】该问题好像是 DNS 设置的问题，因为可以上 QQ 而不能浏览网页是这类问题的典型病征。然而通过检查却排除了 DNS 方面的原因，同时也可以肯定不是病毒、其它网络设置等方面存在问题。于是拿来一台笔记本进行实验，发现可以正常上网。经过对比，发现唯一的区别就是笔记本用的网卡为 10M 网卡。于是将台式机的网卡设置为 10M 全双工传输模式，问题得到了解决。



修改网卡传输速率

双网卡无法同时接入两个广域网

【故障现象】某邮政营业网点的小型局域网，所有计算机均安装双网卡，其中一块网卡通过路由器和交换机接入邮政系统内部网络（通过广域网接入），网关为路由器的地址。另一块网卡经由交换机通过带路由功能的 ADSL Modem 接入 Internet，其网关为 ADSL Modem 的地址。两块网卡的 IP 地址、子网掩码和默认网关均不同。现在感到疑惑的是，为什么任何计算机都不能同时进入邮政系统内部网络和 Internet？应该怎样解决此问题呢？

【解决方法】同一台计算机的两块网卡拥有不同的 IP 地址和网关，是无法同时接入两个不同的非本地网络的，这里涉及到默认网关的工作原理。默认网关是指当计算机访问非本地网络时，将访问请求转发至该 IP 地址。当一台计算机中同时存在两个网关时，系统将无法确认应该使用哪个网关进行转发，于是就会出现网络不通或连接不稳定的情况。要想解决此问题，下面的两个方案可供参考：

方案一，将路由器更换为包括两个 WAN 端口的型号，使两个 WAN 端口分别连接至邮政系

统内部网络和 ADSL Modem。然后在路由器上设置路由策略，使访问邮政系统内部网络的请求转发至内部 WAN 端口，而其它访问则转发至 ADSL Modem 连接，从而实现 Internet 和内部网络的同时接入。假设内部网络采用 10.114.0.0 网段，默认网关的 IP 地址为 10.114.223.254，子网掩码为 255.255.254.0；连接 ADSL 网卡的 IP 地址为 192.168.0.1，则在路由器中添加如下命令行：

```
ip route 0.0.0.0 0.0.0.0 192.168.0.1
```

```
ip route 10.114.0.0 255.255.254.0 10.114.223.254
```

方案二，如果客户端操作系统为 Windows 2000/XP，可以通过添加路由表的方式实现。在命令提示符下键入如下命令：

```
route add 0.0.0.0 mask 0.0.0.0 192.168.0.1
```

```
route add 10.114.0.0 mask 255.255.254.0 10.114.223.254
```

快速收集局域网计算机网卡 MAC 地址

【故障现象】我是一个刚做网管工作不久的新手，公司规定每周上交一份局域网计算机网卡 MAC 地址的清单。有没有方法可以在服务器上快速收集这些 MAC 地址呢？

【解决方法】这个问题很容易解决，只需借助一款具有查看局域网计算机网络信息的网管工具即可实现。这些工具很多，其中 LANSee（局域网查看工具）就是一款不错的工具。安装并启动该工具，在工具栏上单击“搜索计算机”按钮。稍等片刻即可扫描到局域网中的计算机，其中包括 IP 地址、计算机名、网卡 MAC 地址等信息。记录下这些信息做成报表即可。



搜集局域网计算机网卡 MAC 地址

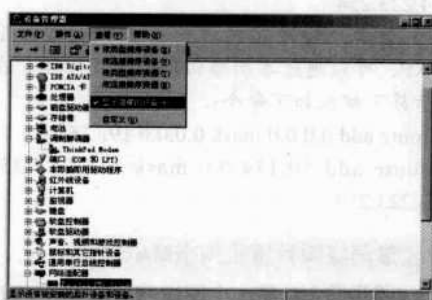
网卡的名称中多了“2#”

【故障现象】某局域网中的一台计算机，在



重新安装网卡后发现网卡的名称比以前多了一个“2#”。请问这是是什么原因造成的？因该如何解决？

【解决方法】这是因为在拔掉旧网卡之前没有能够将其完全卸载所造成的，该网卡的驱动程序仍然保存在系统中，尽管不会影响新网卡的使用，但是会在新网卡的名称中加一个“2#”，用于区别原来的网卡。打开“设备管理器”窗口，然后依次执行“查看/显示隐藏的设备”菜单命令。展开“网络适配器”目录，将新旧网卡全部删除。重新启动计算机并安装新网卡驱动程序即可。



显示隐藏的设备

USB网卡无法正确安装

【故障现象】一台IBM笔记本电脑，使用USB网卡（8139芯片），原来的操作系统为Windows 98，连网正常。升级为Windows 2000系统后，就无法连接网络了，显示网络线缆已经拔出，而且不能Ping通本机IP地址。卸载该网卡后，重新安装网卡和协议并分配地址，但还是不能Ping通。不过，在设备管理器中显示一切正常。请问，如何解决？

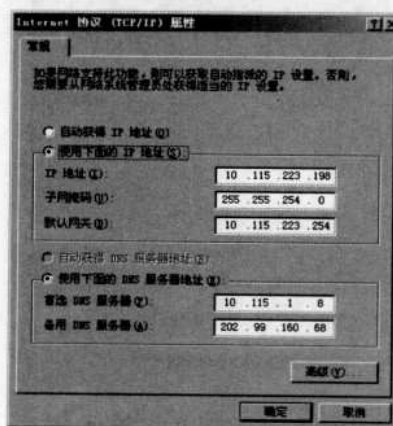
【解决方法】通常情况下，显示网络线缆已经拔出，说明网线没有插好或者网线没有正确连接到集线设备。如果确认网线和网络连接没有问题，则可能是网卡驱动程序的安装有问題。建议在网卡厂商的官方网站上寻找Windows 2000的驱动程序，下载并重新安装该设备的驱动程序。此外，还可下载并安装Windows 2000的Service Pack 4，以修补系统漏洞。如果采用以上方法仍然不能解决故障，建议将系统升级为Windows XP或者更换一个USB接口。

安装网卡后启动速度变慢

【故障现象】为计算机安装网卡连入局域网后，系统启动速度比原来慢了很多。局域网采用DHCP

动态分配IP地址，因此客户端计算机采用自动获取IP地址的方式。请问，应该如何解决启动速度变慢的问题？

【解决方法】安装网卡后计算机的启动速度变慢是正常现象，因为系统启动时除了需要检测网络连接外，还会自动检测网络中的DHCP服务器，增加了系统的启动时间。如果想要加快系统的启动速度，就应当为计算机指定静态的IP地址，以减少系统的检测时间，而不是采用自动获取IP地址的方式。



指定静态IP地址

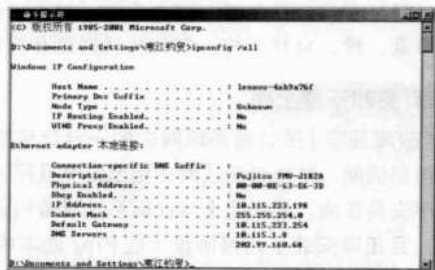
网卡MAC地址异常

【故障现象】一个小型局域网采用交换机进行连接，其中有一台运行Windows XP操作系统的计算机不能正常连接网络。各项网络参数设置均正确，在用“ipconfig /all”命令检查网络配置信息时，显示网卡的MAC地址是“FF-FF-FF-FF-FF-FF”。请问这是不是正常的，应该如何解决此问题？

【解决方法】从“ipconfig /all”的返回结果来看，应当是该计算机的网卡出现故障，因为网卡的MAC地址不应当是“FF-FF-FF-FF-FF-FF”这样的字符串。网卡MAC地址由12个十六进制数来表示，其中前6个十六进制数字由IEEE（美国电气及电子工程师学会）管理，用来识别生产者或者厂商，构成OUI（Organizational Unique Identifier，组织唯一识别符）。后6个十六进制数字包括网卡序列号或者特定硬件厂商的设定值。显示“FF-FF-FF-FF-FF-FF”则说明该网卡存在故障，由此导致使用该网卡的计算机不能正常连接

第十四章 局域网故障排除实例

局域网，建议为故障计算机更换一块新网卡后再进行测试。



执行“ipconfig /all”命令

多种方法解决网卡冲突故障

[故障现象] 完成网卡的安装后，有时常常因为跟系统中的其它设备发生冲突而导致网卡或其它设备不能正常工作。

[解决方法] 这种冲突的产生通常跟系统的默认设置有关，而不能简单地误认为是网卡问题。遇到网卡冲突问题可从以下几个方面尝试解决：

(1) 升级操作系统。版本较新的操作系统往往拥有更好的兼容性和更稳定的性能，对各式网卡的自动识别程度也较高。例如 Windows XP/Sever 2003 等系统，都能更为合理地分配和识别系统硬件资源。

(2) 重新分配系统资源。新安装的网卡可能使用了已有设备的 DMA 通道、I/O 地址、IRQ 中断等系统资源，这会引发网卡“冲突”故障。此时需要为新网卡手动分配一个不同的资源就能解决冲突。首先应该打开“设备管理器”窗口，右键单击网卡图标并执行“属性”快捷命令，打开网卡属性对话框。切换至“资源”选项卡，对网卡的“输入/输出范围”、“中断请求”等资源重新进行设置以免出现重复。

注意

在修改网卡资源前最好先查明究竟是什么类型的资源与其它设备发生了冲突，以及哪些资源还可以使用，然后才能为有问题的网卡设备重新指定资源。如果无法在“资源”设置界面中更改设置，可以重新启动系统进入“安全模式”，然后在安全模式下尝试打开“设备管理器”的“资源”设置界面，并取消对“使用自动设置”的选择，一般可以更改设置。



重新设置系统资源

(3) 屏蔽无用设备。也许有些硬件设备用户平时很少用到，可以考虑屏蔽这些系统设备让出占用的系统资源。譬如默认情况下 COM2 端口使用中断“IRQ3”，而网卡也默认使用“IRQ3”，这样就使得网卡与 COM2 端口经常发生“冲突”。用户只要将 COM2 端口屏蔽掉就能让网卡独自享用“IRQ3”中断，这样就可避免冲突。

在设备管理器窗口中屏蔽 COM2 端口时，可在网卡属性窗口的“常规”选项卡中，将“设备用法”设置为“不要使用这个设备（停用）”就可以了。



屏蔽有关设备

网线短路导致网络通信中断

[故障现象] 某单位局域网建成并使用的的时间较长，最近发现其中一台计算机经常出现丢包现象，且丢包数量不固定。用网线测试仪检测该计算机的物理链路，发现网线中的白橙线和白蓝线发生了短路。请问如何在不重新布线的前提下排除故障并达到 100Mbps 的传输速度？



【解决方法】可以通过改变线序来解决此问题。对于 100Base-TX 的局域网络只用到了双绞线中的 2 对线来传输信号，分别与水晶头上的 1、2、3、6 线相对应，而对应的双绞线颜色则依次是白橙、橙、白绿、绿。既然白橙线和白蓝线发生了短路，只需放弃白橙和橙这一对双绞线，并用白棕线和棕线代替即可。重新压制后的线序应该是：白棕、棕、白绿、空、空、绿、空、空，且网线两端都应该按此顺序压制。

延长网线的距离

【故障现象】单位办公室没有安装网络模块，网线从机房引出后直接插接在网卡上。现在办公室的电脑桌因故需要移动几米，而网线长度不够长。请问有什么方法能够解决网线不够长的问题呢，直接剪断网线进行连接行不行？

【解决方法】将网线的水晶头剪断再接出一段网线的做法显然是不行的，因为这样做会破坏网线的电气特性，使数据传输的误码率大大增加。建议购买一个两头均是 RJ45 接口的 RJ45 连接器，然后再做一根足够长的网线进行连接即可。



RJ45连接器

双机直连无法共享上网

【故障现象】办公室的两台计算机，其中一台计算机安装双网卡。现准备进行双机直连并实现 Internet 连接共享，可是使用普通网线连接两台计算机后，用于双机直连的网络连接总是提示“网络线缆没有插好”。而与 ADSL Modem 相连的网络连接显示正常，更换网卡和网线故障依旧。请问这是什么原因造成的？

【解决方法】根据故障描述可以断定是双机直连所使用的网线有问题。用于双机直连的网线应当使用交叉线，而不能使用直通线。普通的网线一般都按照 568B 标准做成直通线，因此不能实现双机直连。解决该问题的方法很简单，只需将用

于双机直连的网线换成交叉线就即可。交叉线的线序应遵循此规则：一端为白橙、橙、白绿、蓝、白蓝、绿、白棕、棕，另一端为白绿、绿、白橙、蓝、白蓝、橙、白棕、棕，需按此规则进行压制。

网卡灯亮却不能上网

【故障现象】某公司局域网内的一台计算机无法连接局域网。经检查确认网卡指示灯亮且网卡驱动程序安装正确。另外网卡与任何系统设备均没有冲突，且正确安装了网络协议（能 Ping 通本机 IP 地址）。最容易产生这种故障现象的原因是什么，应该如何解决呢？

【解决方法】从故障描述的情况来看，网卡驱动程序和网络协议安装不存在问题，且网卡的指示灯表现出正常的现象，因此可以判断故障原因可能出在网线上。因为网卡指示灯亮并不能表明网络连接没有问题，譬如 100Base-TX 网络使用 1、2、3、6 两对线进行数据传输，即使其中一条线断开后网卡指示灯也会点亮，但是网络却不能通信。建议使用网线测试仪检查故障计算机的网线，如果网线正常则尝试能否 Ping 通其它计算机。如果不能 Ping 通可更换集线设备端口再试验，仍然不通时可更换网卡。

14.2 路由器、交换机故障排除实例

用路由上网无法语音聊天

【故障现象】单位的小型办公网络，准备使用带路由功能的 ADSL Modem+ 交换机实现共享接入 Internet。成功接入 Internet 后能够正常浏览网页，可以使用 QQ 聊天但不能使用 QQ 的语音功能。每次建立语音连接后对方只能接听一声便用文字告之网络已断，或根本不能接通。请问这是什么原因造成的？

【解决方法】当使用聊天软件进行语音聊天室时，要求至少有一方有合法的 IP 地址。计算机通过路由功能上网时没有合法的 IP 地址，当对方也是通过代理服务器或者使用路由功能上网时也没有合法的 IP 地址。当拥有合法 IP 地址且防火墙没有关闭相应的端口时，即可进行语音通话。

路由器拒绝服务

【故障现象】登录路由器管理界面后很快出

第十四章 局域网故障排除实例

现提示信息“Denial of service attack from 61.149.185.54 is finished”, “Denial of service attack from 218.80.104.168 is under way”, 并且持续显示，请问这是怎么回事？

【解决方法】该信息提示路由器的设置不允许用户从广域网登录。用户可以登录到路由器的LAN口进行设置（192.168.x.x、10.x.x.x、172.16.x.x相关的地址）。

宽带路由器共享上网频繁掉线

【故障现象】办公室小型局域网准备采用宽带路由器+交换机+ADSL Modem的方式共享上网。路由器设置成自动连接模式，上网时总是出现瞬间掉线情况（大约每隔20分钟掉一次）。查看路由系统日志看到“接收到PADT，服务器端要求断开此次连接”的提示。用单个计算机直接连接ADSL Modem上网无此情况发生。请问引发此故障的原因是什么，应当如何解决？

【解决方法】从故障描述中分析，引发此故障的原因大致有两个方面：一方面可能是路由器的设置存在问题。有的路由器在检测到连接在一定时间内处于空闲状态时自动断开连接，如果是这个问题可以设置为“永不断线”模式。另一个方面可能是ISP（如网通公司、电信公司）通过绑定ADSL Modem的MAC地址的方式限制用户使用路由方式上网，这种情况下可以将ADSL Modem的MAC地址“克隆”到宽带路由器中使用。克隆MAC地址的方法请查阅相关资料。

路由器故障导致掉线

【故障现象】两台计算机使用TP-LINK R410宽带路由器共享上网，连接完成后发现无论哪台计算机先开机上网，当遇到另一台开机时必定会出现掉线现象。此时重新连接可以恢复正常，请问这是是什么原因造成的，应该如何解决？

【解决方法】从故障描述中可以判断是路由器存在物理或设置问题，建议按照以下步骤排除故障：重新启动路由器看故障是否能被排除；检查计算机与路由器的连接是否采用直通线，虽然TP-LINK R410路由器支持自动翻转，不过使用非正常的跳线往往会导致一些故障发生更改为使用代理服务器方式上网，重复两台计算机的开关机操作检测ADSL Modem的连接是否正常，如果发

生异常则表明是ADSL Modem存在问题。

路由器上的Link灯不亮

【故障现象】新搭建的公司办公局域网，完成物理连接后发现一台路由器的Link灯不亮，请问应该如何解决此问题？

【解决方法】路由器上的Link灯代表了它是否处于正常的工作状态。如果Link灯亮起代表联机成功，如果Link灯不亮则代表联机失败或没有连接。通常情况下这个问题是由网线的跳线所导致的。当用户使用路由器连接不同设备的时候，需要进行不同网线的跳线切换，因为直连网线或交叉网线所对应的网络设备并不相同。宽带路由器的背面通常有一个“MDIX”按钮用于负责进行直连网线或交叉网线的切换，如果Link没有亮起，可以按下该按钮尝试解决问题。

华为ar28-09b路由器删除路由

【故障现象】局域网中的一台“华为ar28-09b”路由器，在往路由表里添加了一个路由后又想删掉它，请问应该怎么删除？

【解决方法】登录路由器管理界面后执行命令“undo route-static x.x.x.x x.x.x.x”即可。

文件共享响应太慢

【故障现象】某单位办公局域网，以前用HUB上网的时候各台计算机之间可以顺利进行文件共享。添加路由器后出现了怪现象，在“网上邻居”中可以看到其它计算机的共享文件，但是将这些共享文件复制到本地计算机时速度奇慢，有时甚至会停止响应。而其它计算机之间的共享是正常的，请问怎么回事呢？

【解决方法】故障描述中提到其它计算机间共享正常，说明问题应该出在本地计算机到路由器端口这一部分连接。这部分连接可能存在的故障包括交换设备端口、网线、网卡和计算机，建议采用替换法尝试解决问题：

- (1) 检查网线的质量及接口是否有问题；
- (2) 改变交换设备端口看能否解决问题；
- (3) 检查网卡驱动程序安装、设置是否正常。计算机是否安装了防火墙软件以及是否正确设置了IP规则；
- (4) 替换计算机的网卡看能否解决问题。



交换机端口不正常

【故障现象】某单位内部局域网的一台 24 口可网管交换机，将计算机连接到该交换机的一个端口后不能连接局域网。但只要换个交换机端口就能正常连接，而且这个存在问题的交换机端口偶尔又能与计算机建立正常的网络连接。请问这是是什么原因造成的？

【解决方法】如果计算机与交换机某端口连接的时间超过了 10 秒钟仍无响应，那么就已经超过了交换机端口的正常反应时间。这时如果采用重新启动交换机的方法就能解决这种端口无响应问题，那么说明是交换机端口临时出现了无响应的情况。不过如果此问题频繁出现而且限定在某个固定的端口，那么建议闲置该端口或更换交换机。

更换交换机后无法上网

【故障现象】某学校局域网通过路由器接入 Internet，其中一台计算机在使用 10Mbps 集线器连接时能够正常连接局域网和 Internet。更换 10/100Mbps 自适应交换机后，虽然系统托盘上显示网络连接正常，却无法连接到 Internet。无论是让路由器分配 IP 地址还是指定静态 IP 地址都不能连接。请问应当如何处理此故障？

【解决方法】遇到此类故障一般可以从以下几个方面进行检查：

(1) 为故障计算机指定一个静态的 IP 地址，该 IP 地址必须与局域网其它计算机位于同一个网段，并采用相同的子网掩码、默认网关和 DNS。当然必须确保不能与其它计算机的 IP 地址发生冲突。

(2) 使用 Ping 命令 Ping 网络内的其它计算机，确认网络连接是否正常。如果能够 Ping 通说明网络连接没有问题，否则故障发生在本地计算机与交换机的连接上。应当使用网线测试仪检查相应网线的连通性。

(3) Ping 路由器内部 IP 地址，如果能 Ping 通说明路由器存在 IP 地址分配故障，极有可能是因为 IP 地址池内的 IP 地址数量过少造成的。如果不能 Ping 通则说明物理链路发生故障，应当检查相应的物理连接。

具体到本例的故障描述，在 10Mbps 网络中可以正常接入，但连接至 100Mbps 交换机时无法通讯，因此可以怀疑连接该计算机的跳线有问题，或者没有按照 T568A 或 T568B 的标准压制网线。

建议使用网线测试仪测试连接该计算机与交换机的跳线的连通性。

更换交换机后下载速率猛增

【故障现象】某单位局域网计算机共享接入 Internet，在使用 10Mbps 的 HUB 连接局域网时，Internet 下载速率仅为 60KB/s。将 HUB 换成交换机后 Internet 下载速率猛增并稳定在 244KB/s。这是不是更换交换机后收到的效果呢？

【解决方法】跟 HUB 相比，交换机可以明显改善局域网的通讯效率。当多个端口同时通信时，交换机可以保证每个端口都可以独享带宽且传输速率不会受到影响。而由于 HUB 是多个端口共享带宽，且同一时刻只能有一对端口进行通信，所以传输速率和传输效率都会受到很大影响。当采用 Internet 连接共享时，如果网络内的计算机数量较多，但 Internet 的并发访问却不多时，使用交换机肯定会在很大程度上改善下载速率。

根据交换机指示灯判断故障

【故障现象】某局域网中的计算机无法在“网上邻居”中看到其它计算机，也无法 Ping 通任何计算机，只能看到并 Ping 通自己。检查与该计算机相连接的交换机端口时，发现 LED 指示灯熄灭。请问应当如何解决此类故障？

【解决方法】对于交换机而言，无论是光纤端口还是 RJ45 端口，每个端口都有一个 LED 指示灯用于指示端口是否处于工作状态。通过指示灯可以判断连接至该端口的计算机或网络设备是否处于工作状态，以及物理链路是否完好。只有该端口所连接的设备处于开机状态且物理链路完好，则端口指示灯才会被点亮。如果连接计算机或网络设备的端口不亮，表明物理链路存在故障。导致本例故障的原因可能是网线连通性故障、物理链路接触不良或者集线设备端口故障。建议更换一条网线，或者使用网线测试仪测试整条链路的连通性。

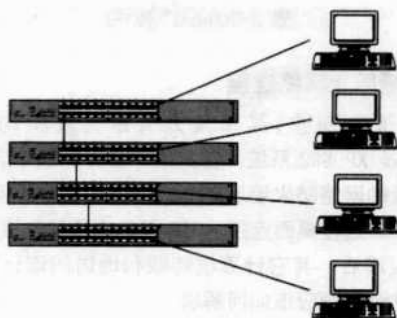
违反 5-4-3 规则导致网络不通

【故障现象】为了满足教学需要，某学校最近建立了一个简易教师机房。出于成本考虑，其网络设备全部采用淘汰下来的 10M 集线器，48 台计算机通过双绞线和 4 台串接的集线器构成了共享式网络。完成网络参数的配置进行联网测试时，发现机

第十四章 局域网故障排除实例

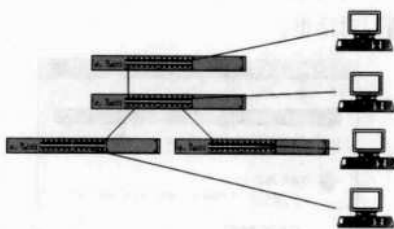
房中的四十多台计算机之间彼此失去了联系。请问这是怎么回事，应当如何解决此问题？

【解决方法】根据故障描述可以看出此故障明显是由于违反了 10Base-T 的 5-4-3 规则，导致的网络故障。所谓 10Base-T 的 5-4-3 规则，是指任意两台计算机之间最多不能超过 5 段线（包括集线器到集线器的连接线缆，也包括集线器到计算机之间的连接线缆）、4 台集线器，其中只能有 3 台集线器直接与计算机或网络设备连接。这是 10Base-T 网络所允许的最大拓扑结构和所能级联的集线器层数。其中，安装在中间的集线器是网络中惟一不能与计算机直接连接的集线器。计算机发送数据后，如果在一定时间内没有得到回应，那么将认为数据发送失败。



违反 5-4-3 规则的网络拓扑

因此只需对集线器的连接方式略做改变就能解决此问题。将其他 3 台集线器都连接在同一台集线器上（此台集线器只能连接其他集线器，不能连接计算机）即可。



改变连接方式

物理链路不通导致不能连接局域网

【故障现象】某单位的综合布线完成后实现了计算机之间的互联，后来扩充计算机数量后，做了

一条网线将计算机连接至信息插座。结果发现无法连接局域网，可以 Ping 自己但不能 Ping 通其它计算机和默认网关，在“网上邻居”中也只能看到自己。请问这可能是什么原因引起的，应当如何处理？

【解决方法】综合布线只是实现链路的铺设，要想实现计算机与网络设备的连接，除了需要用网线连接计算机与信息插座外，还必须用跳线连接配线架与网络设备。配线架上的每个端口都对应一个信息插座，只有将该端口连接至集线设备才能将计算机连接至网络。

集线设备与配线架的连接以及计算机与信息插座的连接所使用的跳线全部都是直通线，事实上，综合布线中的水平布线只是在某种意义上对跳线的延长。需要注意的是，10Base-T 和 100Base-TX 网络只是使用双绞线 4 对线中的 2 对，即 1、2 线对和 3、6 线对，而 1000Base-T 网络则使用双绞线的全部 4 对线。因此在连接网络时，一定要使用网线测试仪测试整条链路，保证 8 条线必须全部连通。

14.3 网络连接故障排除实例

限制客户机的上网速度

【故障现象】某学校几个寝室的计算机组成一个局域网，通过 ADSL 方式接入 Internet。将其中一台运行 Windows XP 的计算机作代理服务器，其它计算机通过代理服务器实现 Internet 连接共享。请问如何才能限制客户计算机的上网速度？

【解决方法】本例中所提到的通过 Windows 系统内置的 ICS 虽然可以实现 Internet 连接共享，却无法实现对客户端的限制。因此要想实现对客户端的高级管理（带宽限制、访问限制），必须借助于“WinGate”或“SyGate”等第三方代理服务器软件。

划分网段限制网络通信

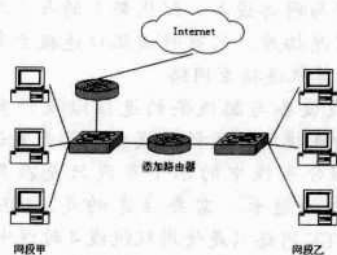
【故障现象】某单位有两个办公室，每个办公室均拥有多台计算机。办公室甲的计算机通过宽带路由器实现共享上网，办公室乙的计算机使用交换机联网，并级联到办公室甲的交换机实现共享上网，两个办公室的计算机可以互相访问。考虑到办公室甲中计算机的安全性，现在希望两个办公室的计算机不能互相访问，但是办公室乙的计算机又能上网。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



请问应该如何实现这一目的?

【解决方法】根据问题描述可拟定划分网段的方案来实现上述目的。将两个办公室的计算机设置为不同的网段，然后在办公室乙中添加一个作为代理服务器的宽带路由器。这样既可以限制两个办公室的计算机进行互访，也可以使两个办公室的计算机都能上网。



设置网段并添加路由器

VPN连接导致工作组计算机不能访问

【故障现象】通过 VPN 连接成功连接至远程局域网中的主机后,可以打开该主机所在局域网中“网上邻居”上的其它计算机。但是本地计算机却不能访问本地局域网工作组中的计算机,不过在断开 VPN 连接后又可以恢复访问。请问这是什么原因造成的?

[解决方法] 涉及 VPN 连接的问题一般比较复杂, 本例故障所提出的问题应该是在本地计算机连接 VPN 服务器后其默认网关被改变, 因此无法访问本地工作组中的计算机。断开 VPN 连接后默认网关又被恢复, 因此又可以继续访问。

网络连接不正常

【故障现象】某公司局域网的计算机全部运行 Windows XP 操作系统，最近其中一台计算机出现网络连接问题，具体表现为：收发邮件、上网都没有问题，但通过 IP 地址和计算机名都不能访问该计算机，提示“不能访问网络位置”。该计算机也不能访问局域网内别的计算机。请问此类问题应该如何解决？

【解决方法】首先检查工作组名或域名是否正确；其次检查局域网内是否有同名的计算机；同时还要检查一下是否禁用了“Guest”账户，以及

检查“本地安全策略/本地策略/用户权利指派/拒绝从网路访问这台计算机”列表中有没有 Guest 项, 如果有的话将其删除。最后还要用最新版本的杀毒软件对系统进行病毒查杀。



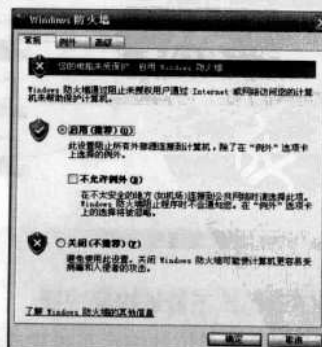
删除“Guest”账户

防火墙阻止网络连接

【故障现象】某单位办公用计算机均运行 Windows XP SP2 系统。在其中一台计算机中启用系统内置的网络防火墙后，其它计算机不能访问该计算机（如远程桌面连接、FTP 服务均不能连接）。关闭防火墙后，其它计算机能顺利地访问该计算机。请问这个问题应该如何解决？

【解决方法】该问题很明显是由于没有正确设置防火墙所致的，只要在防火墙中允许相关服务连接即可。具体操作步骤为：

STEP 1 在“网络连接”窗口右键单击已启用防火墙网络连接图标，执行“属性”快捷命令，打开“本地连接 属性”对话框。切换至“高级”选项卡，并单击“设置”按钮，打开“Windows 防火墙”对话框。



“Windows防火墙”对话框

第十四章 局域网故障排除实例

STEP 2 单击“高级”标签，在“高级”选项卡中单击“网络连接设置”区域的“设置”按钮，打开“高级设置”对话框。在“服务”列表中选择相应的服务复选框，并连续单击“确定”按钮使设置生效。

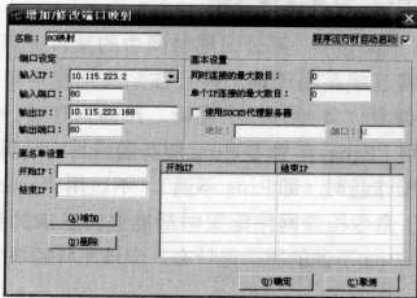


选取相关服务

如何进行端口映射

[故障现象]某学校局域网代理服务器的内部IP地址为“10.114.223.2”，现准备将该服务器上的“80”端口映射到一台IP地址为“10.114.223.168”计算机的“80”端口。请问使用什么方法最容易实现？

[解决方法]可以使用一款名为“PortMap”的小工具来实现。将该软件安装到服务器上，然后再设置好进入的端口和映射到的IP和端口即可。



设置映射属性

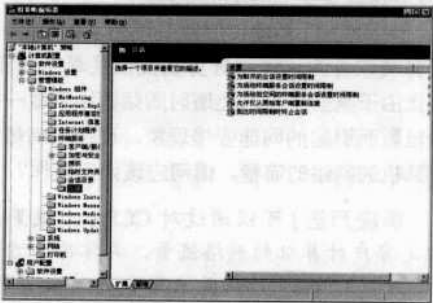
远程桌面连接超出最大连接数

[故障现象]某单位服务器运行 Windows Server 2003 系统，在使用“远程桌面连接”功能远程控制服务器时出现“终端服务超出最大允许连

接数”的提示，从而导致无法登录。请问导致该问题的原因是什么，应当如何解决？

[解决方法]因为在 Windows Server 2003 服务器中设置了最大允许连接数。当用户在结束远程连接没有注销而直接关闭了远程桌面窗口时会导致连接数超过最大连接限制。可以在“组策略”中设置时间限制来解决该问题，操作步骤如下：

STEP 1 依次单击“开始运行”，在“运行”编辑框中键入“gpedit.msc”命令并回车，打开“组策略”窗口。在左窗格中依次展开“计算机配置/管理模板/Windows 组件/终端服务”目录，并选中“会话”选项。



选中“会话”选项

STEP 2 在右窗格中双击“为断开的会话设置时间限制”选项，打开“为断开的会话设置时间限制 属性”对话框。点选“已启用”单选框，在“结束断开连接的会话”下拉菜单中选择时间1分钟。单击“确定”按钮使设置生效。



其实最好的解决方法还是通过注销的方式断开远程桌面连接。

无法Ping通计算机名

[故障现象]某公司局域网拥有50多台计算机，在客户计算机上可以用Ping命令Ping通其它计算机的名称。而其中一台计算机只能Ping其IP地址才能Ping通，Ping其计算机名时不能Ping通。请问这是什么原因造成的？

[解决方法]在局域网中，计算机名是通过



NetBIOS 浏览器选举主浏览器后，所有同意该选举的计算机向主浏览器登记名字建立起来的表项。假如某台计算机因为其它原因不同意该选举，那么就可能会产生多台不相容的主浏览器。一台计算机只能向一个主浏览器登记名字，当在甲主浏览器中登记名字的计算机试图联系在乙主浏览器中登记名字的计算机时是不能成功的，当然也不能直接 Ping 通，但可以通过 IP 地址进行通信。另外 TCP/IP、IPX 等协议都可以支持 NetBIOS，但基于 TCP/IP 的计算机跟基于 IPX 的计算机也不能互相 Ping 通 NetBIOS 名称。在统一的 TCP/IP 环境中可以通过部署 WINS 服务来避免这个问题。

在代理服务器上限制网络流量

【故障现象】某单位服务器使用“CCproxy”代理服务器软件为局域网计算机提供共享上网服务。为防止由于某些员工在上班时间频繁地下载一些软件和电影而引起的网速变慢现象，现在限制每台客户计算机的网络流量。请问应该如何操作？

【解决方法】可以通过对 CCProxy 设置来限制指定客户计算机的网络流量，具体操作方法如下：运行 CCProxy 并在其主窗口中单击“账号”按钮，在打开的“账号管理”对话框中，单击选中“属性”区域“允许范围”下拉菜单中的“不允许部分”选项。



“账号管理”对话框

单击“新建”按钮，打开“账号”对话框。在“IP 地址/IP 段”编辑框中输入要限制客户计算机的 IP 地址；接着将“最大连接数”设置为“1”，这表示只允许该客户机同时建立一个连接，这样限制一些下载工具软件的多线程数目；最后将“带宽（字节/秒）”设置为“50”，这表示该限制的客户机的带宽上限为 50kB/s。最后连续单击“确定”按钮使设置生效。



设置账户限制属性

限制局域网和外网间的流量

【故障现象】某单位局域网划分为两个子网，并通过一台服务器和外网进行连接。现在其中一个子网与外网间流量太大，严重影响了另一个子网的正常工作。现在想限制该子网的网络流量，请问通过什么方法可以实现上述目的？

【解决方法】根据问题描述，建议用户在服务器上安装一个名为“网路岗”的工具软件来实现上述目的。该软件可以监控整个局域网的网络活动，其中包括限制局域网与外网的流量。在软件的“监控策略”对话框中，选中“基于‘网卡’”、“基于‘账户’”或“基于‘IP 地址’”选项的任意一项复选框，然后选中要限制流量的计算机，最后选中“限制流量”标签并设置该计算机的流量大小即可。当超过这个流量大小时，被限制的计算机将被自动断开连接。

无法 Ping 通其他计算机

【故障现象】某公司局域网中的某台计算机可以正常连接至局域网，并且在系统托盘中可以显示 100M 的“本地连接”图标。然而当在该计算机上使用“Ping”命令 Ping 服务器或其它计算机时显示操作超时（即 Ping 不通）。不过用“ipconfig/all”命令检查网络配置时却能返回正常的参数。请问 Ping 不通的原因是什么，应该怎样解决？

【解决方法】根据问题描述可以初步判断是由于该机禁用了“ICMP”导致。而禁用 ICMP 的方法有很多种，例如通过安装个人防火墙或者设置 IP 数据包筛选器均可以实现。当“ICMP”被禁用时，尽管无法 Ping 通其它计算机，但使用 IE 浏览器上网或进行 FTP 访问是没有问题的。禁用“ICMP”的目的是防止计算机遭受基于 Ping 命令

第十四章 局域网故障排除实例

的“DDOS”攻击，因此一般的防火墙软件默认都会禁用掉“ICMP”。解决该问题的方法就是重新设置防火墙规则，启用“ICMP”。然而这样做容易使计算机遭受恶意攻击，从而带来安全隐患。



瑞星个人防火墙禁止ICMP

IP地址与系统硬件冲突

【故障现象】某单位办公室的计算机运行 Windows 98 系统，最近经常出现“系统探测到 IP 地址 10.114.223.198 与系统硬件地址 00:00:0E:63:E6:3D 冲突”的提示框。有时连续出现好几个这样的提示框，如果不关闭这个提示框则其它的一切操作都将无法进行。请问这是是什么原因造成的，应该如何解决？

【解决方法】这种情况是由于本机 TCP/IP 协议中设置的 IP 地址与局域网中另外一台计算机或网络设备的 IP 地址发生冲突所致的。发生冲突的 IP 地址显然就是“10.114.223.198”，系统硬件地址“00:00:0E:63:E6:3D”是另一台计算机网卡或其它网络设置的 MAC 地址。因为已经有其它网络设备的 MAC 地址“00:00:0E:63:E6:3D”绑定了“10.114.223.198”这个 IP 地址，所以本机网卡 MAC 地址若再次绑定这个 IP 地址的话是无效的，因此会出现 IP 地址与系统硬件有冲突的提示。

解决该问题的方法就是更改本机的 IP 地址，或者如果本机对“10.114.223.198”这个 IP 地址有合法使用权，那么应该更改另一台计算机的 IP 地址。总之，每一个 IP 地址在同一个网络中应当具有惟一性，绝不能重复设置。

14.4 网络设置故障排除实例

更改“远程桌面连接”的默认端口

【故障现象】某单位局域网服务器运行 Windows Server 2003 系统。使用“远程桌面连接”功能时发现，一旦要求远程连接服务器的桌面，其系统自

带的防火墙就会自动打开“3389”端口。为了保证服务器系统的安全，请问能不能在不打开“3389”端口的情况下使用“远程桌面连接”功能？

【解决方法】通过更改“远程桌面连接”默认端口的方式达到目的。在注册表中修改该端口的方法为：打开“注册表编辑器”窗口，分别展开“KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp”和“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp”分支，在这两个分支下面均有一个“PortNumber”项，将该项的“十进制”值改为其它数值（如 5793）值即可。

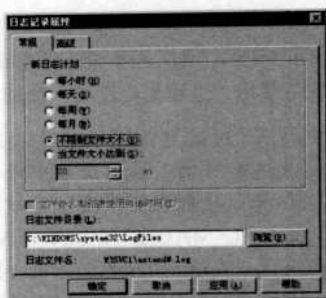


修改“PortNumber”项的数值

限制日志大小导致Web服务自动停止

【故障现象】某单位服务器运行 Windows Server 2003 系统。近来发现只要系统中的某个日志文件体积达到 512KB，Web 服务将自动停止，只能重新启动系统才能启动 Web 服务。请问这个问题时如何造成的，应该如何解决？

【解决方法】根据故障描述来判断，很可能是在 IIS 6.0 中限制了日志文件的大小而导致故障发生的。可以取消这种限制来解决问题，具体操作方法为：打开“Internet 信息服务 (IIS) 管理器”窗口，在左窗格中依次展开“ServerName/网站”目录。右键单击 Web 站点名称，执行“属性”快捷命令。在打开的 Web 站点属性对话框中切换至“网站”选项卡，然后在“启用日志记录”区域中单击“属性”按钮。在打开的“日志记录属性”对话框中点选“不限制文件大小”单选框，连续单击“确定”按钮即可。



取消日志文件大小限制

无法使用服务器列表

【故障现象】某学校局域网计算机运行 Windows XP 系统，使用“网上邻居”窗口中浏览局域网计算机时长时间没有反应，最后弹出提示框：“XXX 无法访问，此工作组的服务器列表当前无法使用。”请问这是是什么原因造成的，应该如何解决？

【解决方法】根据故障描述中提到的“此工作组的服务器列表当前无法使用”提示框可以判断出工作组“XXX”处于无法访问的状态。如果在“命令提示符”窗口中执行“Net view”命令的话，可以发现这个错误的代码是“6118”。该代码表示工作组的浏览功能出现了意外终止，解决方法是在“命令提示符”窗口中执行“net start “computer browser””（computer browser 两端需要有双引号）命令启动相应的浏览服务即可。

在局域网中隐藏特定计算机

【故障现象】某单位办公局域网，客户计算机全部运行 Windows XP 系统。其中一台计算机具有特殊用途，为防止别人在“网上邻居”中看到该计算机，准备将其在“网上邻居”中隐藏起来。请问应该如何操作才能达到这一目的？

【解决方法】这一目的完全可以事先，可按以下两种方案操作操作：

(1) 编辑注册表。展开“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters”分支，新建一个 DWORD 键，命名为“Hidden”，将键值修改为“1”，保存注册表即可。



新建DWORD键隐藏计算机

(2) 在“命令提示符”窗口中运行“net config server /hidden:yes”命令，这样用户可以在“网上邻居”地址栏中通过输入\\计算机名或 IP 地址之类的 UNC 路径连接到目标计算机，但不能在“网上邻居”中看到计算机。

查看本地计算机上的连接

【故障现象】某公司刚刚组建了局域网，为了防止恶意攻击想随时知道有哪些计算机正在连接服务器。请问应该如何设置才能获知本地计算机的当前连接呢？

【解决方法】目前的大部分防火墙软件都具有上述功能，当发现系统遭到攻击时会自动报警。用户只要点击相应的提示框就可以启动追踪软件。不仅可以看到攻击源的具体地址，还可以看到它所跳转的各个服务器的相关情况。譬如功能强大的“Norton Internet Security”不仅可以报告是谁在攻击你，而且还可获取攻击源的准确地理位置。另外还可以使用系统内置的“Netstat”命令查看当前连接。在“命令提示符”窗口中执行命令“Netstat -a”即可查看所有与本地计算机相连的外部地址及状态。



执行“Netstat -a”命令

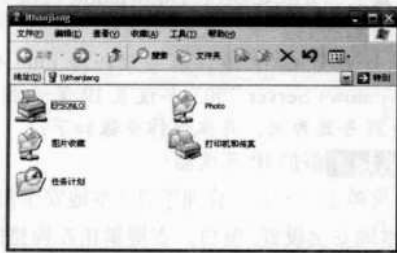
无法用计算机名访问共享资源

【故障现象】某单位局域网一直通过在“运行”

第十四章 局域网故障排除实例

编辑框输入 \\ 计算机名的形式访问其它计算机的共享资源。在为所有的计算机重新安装系统后，发现某一计算机不能通过这种方式访问其它计算机了。当在“运行”编辑框中输入 \\ithanjiang 之类的 UNC 路径时，提示找不到该计算机，而名为 ithanjiang 的计算机可以被其它计算机访问。首先可以排除网络物理连接存在问题，请问遇到此类问题应当如何解决？

【解决方法】故障描述中提到是在重装系统后出现的问题，因此首先应该检查网卡驱动程序或网络协议是否正确安装，IP 地址是否正确设置。如果 IP 地址设置没有问题且已经安装网卡驱动程序，建议在“设备管理器”中删除网卡驱动程序后重新安装。如果计算机运行 Windows 9X 系统，则“NetBEUI”协议是一定要安装的。如果所有的网络协议均没有问题，通过 UNC 路径应该可以访问目标计算机。



通过UNC路径访问共享资源

添加IPX/SPX协议提示地址相同

【故障现象】某小型办公网络，准备使用其中三台计算机玩对战游戏。为每一台计算机添加 IPX/SPX 协议后，系统提示地址相同。请问这是为什么，因该如何解决？

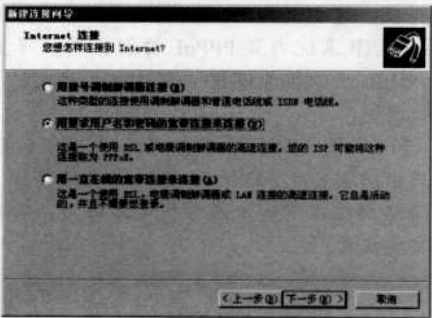
【解决方法】由于使用原有网络中的计算机玩对战游戏，因此可先排除计算机存在 IP 地址冲突、计算机名相同等问题，因此问题主要集中在 IPX/SPX 协议后系统所发生的变化。IPX/SPX 协议无需配置即可直接使用，之所以在玩游戏时提示同一地址，很可能是因为在游戏中创建的名称相同。建议为每个用户创建一个不同的名称，另外下载安装该游戏的联机补丁也能够解决该问题。

PPPoE协议冲突

【故障现象】某小区宽带用户的计算机运行

Windows Server 2003 系统，在使用 LAN 接入方式时能正常上网。后改用虚拟拨号（使用 RASPPPoE）方式上网时出现问题，具体表现为开机上网几分钟后出现无流量的现象，且此时无法断开网络连接，只有重新启动计算机才能恢复正常。经过实验发现，此故障只在 Windows Server 2003 系统中出现，换用其它系统则是正常的。请问这是是什么原因造成的，应该如何解决？

【解决方法】Windows Server 2003 和 Windows XP 系统均内置 PPPoE 协议，建议直接在系统中创建虚拟拨号连接。本例故障的原因极有可能是第三方拨号软件跟系统产生冲突造成的，卸载第三方拨号软件而改用系统自带拨号连接。



创建PPPoE拨号连接

IPX/SPX协议导致网络连接中断

【故障现象】某公司的专业管理系统在升级版后发现各客户端的数据连接常常中断，只能在重新启动计算机后才能再次连接。该公司的服务器型号较老，运行 Windows NT4.0+IE 4.0 系统，客户端计算机运行 Windows 98 SE+IE4.0 系统。该管理系统说明文档标明只需 TCP/IP 支持，而 Windows NT 4.0 自带 IPX/SPX 兼容协议，且客户端也安装了 IPX/SPX 兼容协议。请问是不是 IPX/SPX 协议导致的故障发生，应该如何解决问题？

【解决方法】在基于“Windows NT + Windows 98”的网络平台中，如果相关软件没有特殊要求只使用 TCP/IP 即可。根据本例故障描述信息，建议删除 Windows NT 和 Windows 98 中的 IPX/SPX 协议。另外需要注意的是，某些专业常常需要较高版本的 IE 浏览器支持。因此建议为 Windows NT 安装最新的 Service Pack，并将所有计算机的 IE 浏览器升级为 IE 5.5 级以上版本。



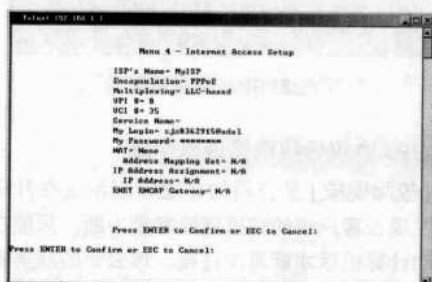
TCP/IP报告错误31

【故障现象】某单位小型局域网准备通过ADSL方式接入Internet。安装ADSL Modem并创建虚拟拨号连接，发现第一次连接没有问题，但断开连接后再次连接时失败，系统提示“TCP/IP报告了错误31：连到系统上的设备没有发挥作用”。重新启动系统可以暂时解决问题，请问这是什么原因造成的，应该如何解决？

【解决方法】根据系统提示信息可以判断故障原因是ADSL Modem与系统兼容性不太好，建议采用以下方法尝试解决：

(1) 升级操作系统。如果作为代理服务器的计算机原有系统为Windows 9X/2000且硬件配置不很低，建议升级为Windows XP系统。并且Windows XP系统内置PPPoE协议，用户可直接创建ADSL虚拟拨号连接，这样会大大减少系统兼容性问题。

(2) 如果ADSL Modem带路由功能，建议启用路由功能实现ADSL Modem的自动拨号。如果不带路由功能则建议添加宽带路由器，实现路由器自动拨号。



启用ADSL Modem的路由功能

启用NetBEUI协议出现网络重名

【故障现象】某公司局域网服务器运行Windows Server 2003系统，由于特殊需要安装了三块网卡并同时连接到同一台交换机，且三块网卡的IP地址在同一网段。查看服务器日志文件，发现了“NetBT”网络重名的记录。请问为什么会出现这种错误提示，应当如何解决？

【解决方法】当计算机安装了两块以上的网卡时是不能安装并启用NetBEUI及其兼容协议的，否则就会产生本例描述中所提到的NetBIOS (NetBT)网络重名故障。此外，将同一计算机上3

块网卡的IP地址设置为同一网段似乎没有意义，除非交换机和网卡均支持并启用了EtherChannel或Port Trunking，从而成倍地扩展网络带宽并实现网络负载均衡。否则的话，同一计算机安装三块网卡通常是为了实现软路由功能，这种情况下必须将3块网卡设置为不同的IP地址段，以实现不同网络间的通信。

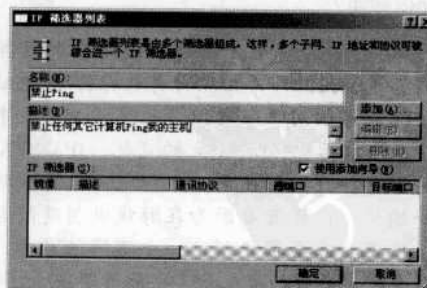
设置IP策略拒绝用户Ping服务器

【故障现象】局域网中为了防止用户频繁Ping服务器而导致服务器性能下降，一般会在防火墙中设置规则拒绝Ping请求。如果单纯借助系统自身的功能是否也可以拒绝用户Ping服务器呢？

【解决方法】频繁地使用Ping命令会导致网络堵塞、降低传输效率，为了避免恶意的网络攻击，一般都会拒绝用户Ping服务器。为实现这一目的，不仅可以在防火墙中进行设置，也可以在路由器上进行设置，并且还可以利用Windows 2000/2003系统自身的功能实现。无论采用哪种方式，都是通过禁止使用ICMP协议来实现拒绝Ping动作。以在Windows Server 2003中设置IP策略拒绝用户Ping服务器为例，具体操作步骤如下：

STEP 1 添加IP筛选器

依次单击“开始/管理工具/本地安全策略”，打开“本地安全设置”窗口。右键单击左窗格的“IP安全策略，在本地计算机”选项，执行“管理IP筛选器表和筛选器操作”快捷命令。在“管理IP筛选器列表”选项中单击“添加”按钮，命名这个筛选器名称为“禁止PING”，描述语言可以为“禁止任何其它计算机PING我的主机”，然后单击“添加”按钮。

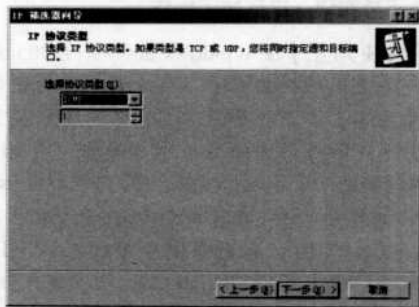


添加IP筛选器

接下来依次单击“下一步/下一步”按钮，选择“IP通信源地址”为“我的IP地址”，单击“下

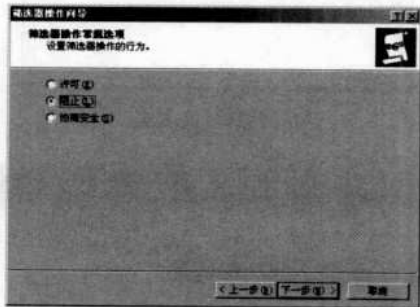
第十四章 局域网故障排除实例

一步”按钮；选择“IP 通信目标地址”为“任何 IP 地址”，单击“下一步”按钮。选择“IP 协议类型”为“ICMP”，单击“下一步”按钮。依次单击“完成 / 确定”按钮结束添加。



选择IP协议类型

然后切换到“管理筛选器操作”选项卡中，依次单击“添加 / 下一步”按钮，命名筛选器操作名称为“阻止所有连接”，描述语言可以为“阻止所有网络连接”，单击“下一步”按钮。点选“阻止”选项作为此筛选器的操作行为，最后依次单击“下一步 / 完成 / 关闭”按钮完成所有添加操作。

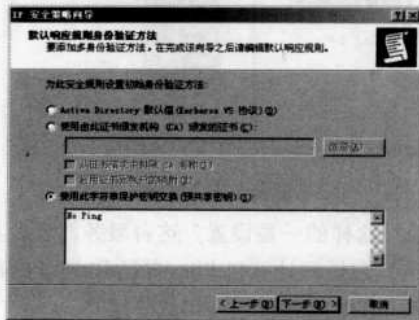


设置筛选器操作的行为

STEP 2 创建 IP 安全策略

右键单击控制台树的“IP 安全策略，在本地计算机”选项，执行“创建 IP 安全策略”快捷命令，然后单击“下一步”按钮。命名这个 IP 安全策略为“禁止 PING 主机”，描述语言为“拒绝任何其它计算机的 PING 要求”并单击“下一步”按钮。然后在勾选“激活默认响应规则”的前提下单击“下一步”按钮。在“默认响应规则身份验证方法”对话框中点选“使用此字符串保护密钥交换”选

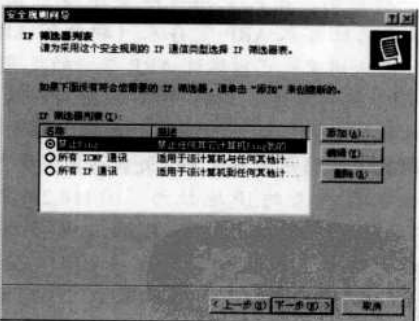
项，并在下面的文字框中键入一段字符串如“NO PING”，单击“下一步”按钮。最后在勾选“编辑属性”的前提下单击“完成”按钮结束创建。



设置身份验证方法

STEP 3 配置 IP 安全策略

在打开的“禁止 PING 主机 属性”对话框中的“规则”选项卡中依次单击“添加 / 下一步”按钮，默认点选“此规则不指定隧道”并单击“下一步”按钮；点选“所有网络连接”以保证所有的计算机都 PING 不通该主机，单击“下一步”按钮。在“IP 筛选器列表”框中点选“禁止 PING”，单击“下一步”按钮；在“筛选器操作”列表框中点选“阻止所有连接”，依次单击“下一步”按钮。取消“编辑属性”选项并单击“完成”按钮结束配置。



选择IP筛选器

STEP 4 指派 IP 安全策略

安全策略创建完毕后并不能马上生效，还需通过“指派”使其发挥作用。右键单击“本地安全设置”窗口右窗格的“禁止 PING 主机”策略，执行“指派”命令即可启用该策略。



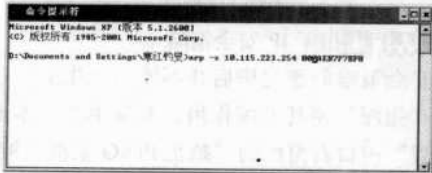
指派IP安全策略

经过这样的一番设置，这台服务器已经具备了拒绝其它任何计算机 Ping 自己 IP 地址的能力了，不过在本地 Ping 自身仍然是通的。

使用ARP绑定默认网关

【故障现象】某单位局域网采用拥有固定 IP 地址的 ADSL 设备接入 Internet，由于经常出现掉线的情况，想在本地计算机中使用 ARP 命令将网关 IP 地址和 MAC 地址绑定。请问这样做能不能解决掉线问题，具体应该如何操作？

【解决方法】通常情况下，ADSL 服务提供商会使用 ARP 协议通过目标设备的 IP 地址查询目标设备的 MAC 地址，以保证通信的顺利进行。在每台安装有 TCP/IP 协议的计算机里都有一个 ARP 缓存表，里面的 IP 地址与 MAC 地址是一一对应的。因此直接将网关 IP 地址相对应的 MAC 地址写入 ARP 缓存表（即使用 ARP 命令绑定默认网关）可以跳过 ARP 查询的步骤，直接从 ARP 缓存表中找到网关 MAC 地址，从而确保通信正常进行。因此采用这种方法可以解决掉线问题，不过用户需要从 ISP 处获得网关的 MAC 地址。假设网关的 IP 地址为“10.114.223.254”，MAC 地址为“00 0A EB 7F 7B F0”，则应该在本地每台计算机上执行命令“arp -s 10.114.223.254 000AEB7F7BF0”。如果网络采用了代理服务器，那么只要在代理服务器中执行该批处理文件即可。

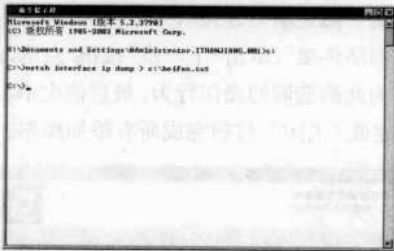


执行ARP绑定操作

备份网络设置

【故障现象】如果能将 IP 地址、网关、DNS、子网掩码等网络设置能像备份文件那样进行备份，当需要重新设置的时候恢复一下就行了。请问这个想法能不能实现，应该如何操作？

【解决方法】在 Windows 2000/XP/2003 系统中有一个使用的网络命令“Netsh”，利用该命令可以对网络设置进行备份，并在需要重新设置时进行恢复。备份的方法为：依次单击“开始/所有程序/附件/命令提示符”，在“命令提示符”窗口中键入命令行“netsh interface ip dump > c:\beifen.txt”并回车。执行该命令可以把 TCP/IP 设置备份到 C 区中名为“beifen.txt”的文本文件中。找到并打开 C 盘的“beifen.txt”文本文件可以查看备份生成的内容，包括 IP 地址、子网掩码、网关、DNS 等网络设置。需要恢复网络设置时只需执行“netsh exec c:\beifen.txt”命令即可。



2-16 备份网络设置

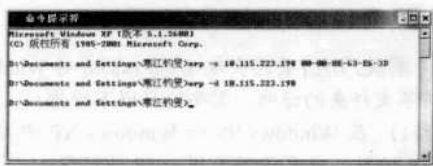
14.5 网络权限设置故障排除实例

禁止客户计算机修改IP地址

【故障现象】某学校机房拥有 60 台计算机，所有计算机均运行 Windows XP 系统。随着学生掌握的计算机操作知识日渐丰富，有些学生经常随意修改 IP 地址，从导致很多计算机无法正常上网。请问能不能禁止学生更改 IP 地址，具体应该如何操作？

【解决方法】只要将每台电脑的 IP 地址和网卡的 MAC 地址进行绑定即可。例如要将 IP 地址“10.114.223.198”与网卡 MAC 地址“00-00-0E-63-E6-3D”绑定，需要在“命令提示符”窗口中执行命令“arp -s 10.114.223.198 00-00-0E-63-E6-3D”。如果要解除绑定，执行命令“arp -d 10.114.223.198”即可。

第十四章 局域网故障排除实例



执行“arp”命令

注意

如果是在 Windows 域环境中，可以使用组策略限制用户修改 IP 地址，并部署 DHCP 服务动态分配 IP 地址。

无访问权限导致共享打印机不能使用

【故障现象】某单位局域网中一台运行 Windows XP SP2 的计算机连接一台惠普打印机，并共享给局域网用户使用。在一台运行 Windows 98 的计算机上使用共享打印机打印时出现提示“写入 \\ithanjiang\HP6L 时出错：访问代码无效。会将打印机设为脱机打印。”请问此故障是什么原因引起的，应当如何解决？

【解决方法】出错提示说明 Windows 98 计算机没有访问 Windows XP 计算机的权限。因为 Windows XP SP2 默认将系统的安全级别设置为最高，因此应当首先确保运行 Windows 98 的计算机能正常访问连接打印机的计算机。然后在防火墙中设置允许共享文件和打印机，并使用 Windows XP 上的用户账户和密码登录。

限制局域网内部指定的计算机上网

【故障现象】某公司若干台计算机组成一个局域网，并使用路由器接入 Internet。现在想通过路由器来限制局域网中部分指定的计算机上网，请问应该怎么操作？

【解决方法】可以先用 MAC 地址扫描软件来扫描那些想限制上网的计算机网卡的 MAC 地址，然后在路由器上使用 MAC 地址过滤即可。这样既不影响内部局域网的使用，又能达到限制目标计算机连接 Internet 的目的。

密码策略导致无法访问共享资源

【故障现象】某单位办公室局域网的计算机全

部运行 Windows XP SP2 系统，其中员工甲为了方便使用为员工乙设置了一个不需要密码即可访问自己的计算机的用户账户。当员工乙使用该空密码账户登录员工甲的系统时却出现访问被拒绝的提示框，而将该账户设置密码后却能够访问。请问造成这个问题的原因是什么，应该如何解决？

【解决方法】这是由于 Windows XP 的安全策略采用了“拒绝优先”的原因造成的。空密码用户通过网络访问使用 Windows XP 系统的计算机时，会出现访问拒绝的现象。用户可以自行取消这种安全策略，具体操作方法为：在“运行”编辑框中键入“gpedit.msc”命令并回车，打开“组策略”窗口。在左窗格中依次展开“计算机配置/Windows 设置/安全设置/本地策略/安全选项”目录，然后在右窗格中双击“账户：使用空白密码的本地账户只允许进行控制台登录”选项，并将其设置为“已禁用”即可。



设置空白密码账户的安全属性

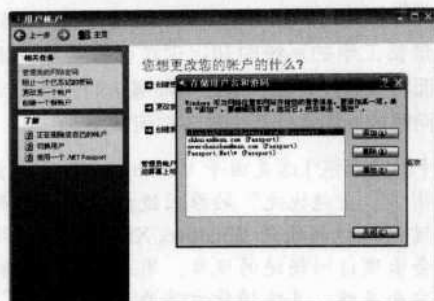
清除访问密码

【故障现象】某公司局域网拥有 50 多台计算机，客户计算机运行 Windows 2000 和 Windows XP 两种操作系统。其中有一台运行 Windows XP 的计算机在访问一台运行 Windows 2000 系统的计算机时要求输入账户及密码，按照提示输入合法的用户名称密码，并勾选了“保存密码”复选框。现在这台 Windows XP 计算机每次都能直接访问那台 Windows 2000 计算机而无须输入密码，请问如何才能删除保存的密码呢？

【解决方法】这个问题属于系统的网络密码问题，可按照如下方法清除保存的密码：依次单击“开始/控制面板”，在打开的“控制面板”窗口中双击“用户账户”图标。打开“用户账户”窗口，单击保存有密码的用户账户，然后单击“管理我



的网络密码”选项，在打开的“存储用户名和密码”对话框中找到相应的密码项并将其删除即可。

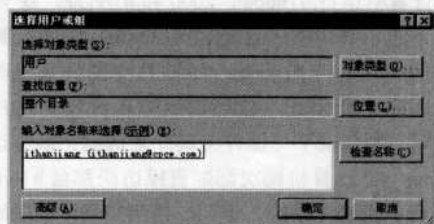


清除指定账户的网络密码

普通用户无法连接远程桌面

【故障现象】由于工作需要，公司需要让一些员工使用远程桌面功能，使他们能够通过自己的电脑远程访问公司的一台 Windows Server 2003 服务器。首先在服务器中为相关人员建立了普通用户账号，当连接远程桌面时出现“此系统的本地策略不允许您交互登录”的提示。请问应该如何设置才能使用普通用户连接远程桌面呢？

【解决方法】这是由于没有赋予该用户远程连接的权限，只需将该用户添加到远程桌面用户组即可。在 Windows Server 2003 服务器的桌面上右键单击“我的电脑”，执行“属性”命令。在打开的“系统属性”对话框中单击“远程”标签，然后单击“选择远程用户”按钮。在“远程桌面用户”对话框中依次单击“添加/高级/立即查找”按钮，然后在用户列表中双击该用户名，并连续单击“确定”按钮即可。



选择“远程桌面”用户

不能正常访问共享资源

【故障现象】某学校局域网，客户计算机分别运行 Windows 98 和 Windows XP 系统。在 Windows 98 系统中访问 Windows XP 系统中的共享资源时提

示不能访问，请问应该如何解决？

【解决方法】要想实现 Windows 98 对 Windows XP 共享文件夹的访问，需要执行以下操作：

(1) 在 Windows 98 和 Windows XP 中安装 TCP/IP 协议，并且设置为同一 IP 地址段；

(2) 在 Windows XP 系统中开启 Guest 账户（取消“账户已停用”复选框），最好在组策略中删除了“拒绝从网络中访问此计算机”中的 Guest 账户；



启用“Guest”账户

(3) 禁用 Windows 98 和 Windows XP 系统中的防火墙。

14.6 其他网络配置故障排除实例

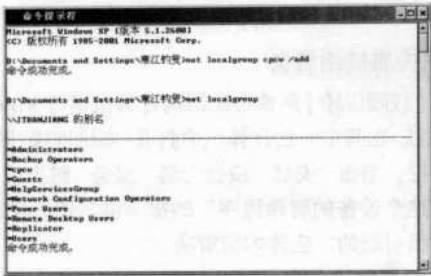
区分 Net localgroup 和 Net group 命令

【故障现象】“Net localgroup”和“Net group”均是对用户组进行操作的命令，请问这两个命令的本质区别是什么，各自有什么功能？

【解决方法】这两个命令分别是对“本地组”和“全局组”进行操作的命令。“全局组”的意思是所建立的组可以在本地和有信任关系的其它域中使用，而“本地组”则只能在本地计算机上使用。与此权限相对应，“Net group”应该在域控制器上使用，建立的组就是“全局组”，该组可以在全域中使用；“Net localgroup”创建的“本地组”只能在本地计算机上使用。例如创建一个普通用户“hanjiangit”，把该用户加入“Users（本地组）”中则只能在本地计算机上使用。如果把“hanjiangit”加入“Domain Users（全局组）”，则该用户就可

第十四章 局域网故障排除实例

以在全域中使用。要创建一个本地组(如“cpcw”),只需在“命令提示符”窗口中执行命令“net localgroup cpcw /add”即可。



创建和查看本地组

列出共享文件信息

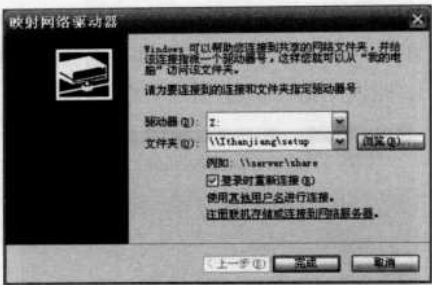
[故障现象] 某公司网络管理员想把局域网中所有计算机中的共享文件、共享打印机等共享信息整理出来，以供所有用户在互相共享文件时使用。请问能不能命令行的方式快速获取这些信息呢？

[解决方法] 可以使用“Net view”命令实现上述目的。在“命令提示符”窗口中使用“CD”命令切换到准备保存共享信息结果的目录，然后键入命令“net view \\lenovo-770b05cc >>shareinfo.txt”。其中“lenovo-770b05cc”为计算机名称，只要将该名称修改为需要查看其共享信息的计算机名称即可。反复执行该命令将所有计算机中的共享信息导入到“shareinfo.txt”文本文件中。

远程运行安装程序失败

[故障现象] 某单位办公网络计算机全部运行 Windows XP 系统，一名用户远程安装 Office 2003 时，系统弹出提示“错误 1606：无法访问网络位置 \\ithanjiang\d\Setup\Office11\”，软件不能完成安装，其中“ithanjiang”是局域网中的一台计算机。请问这是是什么原因造成的，应该如何解决？

[解决方法] 根据故障描述可以很明显的看出，该用户是通过 UNC 共享的方式从网络中另一台计算机远程运行安装程序。解决方法也很简单，只需将完整的安装程序复制到本地计算机或在本地计算机上创建网络驱动器映射，然后再从本地计算机运行安装程序就能解决问题。



映射网络驱动器

利用磁盘挂载解决空间不足问题

[故障现象] 某单位一台基于 Windows server 2003 系统的服务器，配置有 120G 的硬盘，所有分区均为 NTFS 格式。最近由于某种需要准备把 G 区空间追加到空间已不太富余的 C 区。请问如何在损失数据的前提下安全地完成这项操作呢？

[解决方法] 建议采用 Windows server 2003 自带的“可更改卷路径”(Mount，也称磁盘挂载)功能来实现上述目的，实现方法如下所述：

STEP 1 右键单击“我的电脑”，执行“管理”命令，打开“计算机管理”对话框。在左窗格中单击“磁盘管理”选项，然后在右窗格的分区列表中右键单击 G 区并执行“删除逻辑驱动器”命令。这时 G 区成了未指派空间。

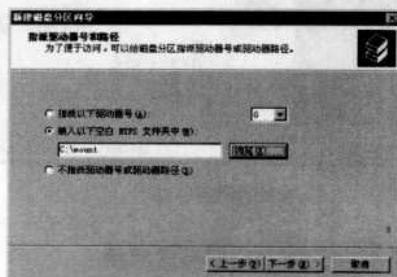


删除逻辑驱动器G

STEP 2 右键单击原来 G 区空间的位置并执行“创建逻辑驱动器”命令。在打开的“创建磁盘分区向导”对话框中连续单击“下一步”按钮，直至出现“指派驱动器号和路径”对话框。点选“将这个卷装入一个支持驱动器路径的空文件夹中”单选框，然后单击“浏览”按钮。在打开的“浏览驱动器路径”对话框中单击 C 区图标，然后单



击“新建文件夹”按钮新建一个文件夹，将文件夹命名为“mount”（注：该文件夹名称可以自由命名）。依次单击“确定/下一步”按钮。



指派驱动器号和路径

STEP 3 在打开的“格式化分区”对话框中勾选“快速格式化”复选框，依次单击“下一步/完成”按钮完成格式化操作。打开 C 区会看到新建的“mount”文件夹的图标是一个磁盘驱动器的图标。表明原 G 区空间已经追加到 C 区了。上述方法 IT 在 Windows 2000/XP 中同样适用。



查看挂接的磁盘图标

网络设备停止响应导致网桥失效

【故障现象】在 Windows XP 中创建网桥后，网桥却不起任何作用，具体表现为任何网络之间的数据通信均无法成功。请问应当如何解决该问题？

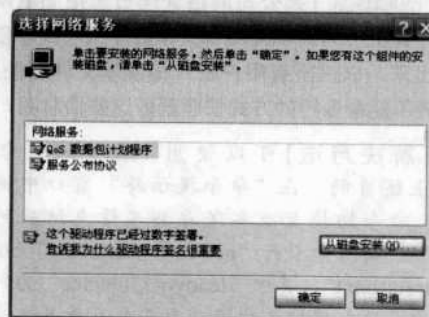
【解决方法】出现这个问题可能是由于某些网络设备不能自动进入网桥所需的“混杂模式”导致的，解决的方法是强制网络设备进入网桥所需的“兼容”模式。在“命令提示符”窗口中执行命令“netsh bridge show adapter”找到停止响应

的网卡标志号，然后执行命令“netsh bridge set adapter 1 forcecompatmode=enable”命令对其进行手工更改即可（其中的“1”是刚才获知的网卡标志号）。

无法安装网络服务

【故障现象】某单位局域网计算机运行 Windows XP 系统，在其中一台计算机中打开“本地连接 属性”对话框。单击“安装”按钮安装“服务”时出现“找不到这个设备的驱动程序”的提示框。请问是什么原因引起的，应该如何解决呢？

【解决方法】出现该提示很可能是要求用户重新指定所安装“服务”的来源，因此只需单击“从磁盘安装”按钮，接着在弹出的对话框中指定来源路径是光盘中的“i386”目录就可以了。



单击“从磁盘安装”按钮

快速获取局域网中计算机的 IP 地址

【故障现象】某公司内部网络拥有 100 多台计算机，为规范管理现在需要获取每台计算机的 IP 地址。请问如何才能快速获取整个局域网中计算机的 IP 地址呢？

【解决方法】可以借助工具软件来解决这一问题。例如“LANSee”、“NetSuper”之类的局域网工具软件均具备该功能。在运行这些工具软件时，首先要确保局域网中所有计算机均为正常联网状态。然后执行搜索操作，很快会在列表中看到包括计算机名称、IP 地址、计算机描述、域/工作组、MAC 地址等信息在内的相关网络信息。